Resisting the Censorship Infrastructure in China

Yubo Kou
Purdue University
kou2@purdue.edu

Yong Ming Kow
City University of Hong Kong
yongmkow@cityu.edu.hk

Xinning Gui
University of California, Irvine
guix@ics.uci.edu

Abstract

China's censorship infrastructure is widely recognized as sophisticated, strict, and comprehensive. We conducted a qualitative study to understand Chinese citizens' practices to navigate the censored Chinese Internet. We found that participants' practices were closely related to their understanding of and resistance to the censorship infrastructure. Participants switched between public and private channels based on the information they desired to seek. They communicated in ways that were considered less vulnerable to censorship examination. They broadened their information search to mitigate the impact of censored content consumption. Through these practices, participants reportedly coped with the censorship infrastructure in an effective manner. We discuss how this case of resistance to censorship in China may further our understanding of such infrastructure.

1. Introduction

China is widely known for its comprehensive, strict Internet censorship infrastructure [23,34]. In a top-down manner, the Chinese central government required that internet companies block keywords, delete unfavorable contents, and ban infringing users [3,21]. By imposing hefty penalties for non-complying organizations, and without providing clear censorship parameters, these entities (e.g., microblogs, news sites, and social-networking sites) are encouraged to develop strict algorithms which filter results with broad strokes, thus resulting in a highly restricted informational spaces [13,21].

We carried out a qualitative study to understand how Chinese citizens resisted the censorship infrastructure. We conducted 32 semi-structured interviews with mainland Chinese citizens, and also observed their discussions on social media. All these interviewees had discussed three recent political events in the Chinese social media: The Umbrella Movement, the National People's Congress, and the crackdown on corruption. By focusing on these highly politicized events, we had opportunities to sample more instances of resistance in our data.

We found that participants' many practices to deal with censorship involved their understanding of how the Internet censorship functioned as an infrastructure. We found a variety of strategies which usually included users attempting to understand boundaries, mechanics, and intents of censorship. In turn, they took measures to avoid, or embrace censorship, hopefully, to make the best of a restrictive informational environment. We discuss the relationship between repression, censorship, and resistance through the infrastructure lens.

2. Background

China has one of the most sophisticated, strict, and comprehensive censorship systems in the world that regulates its Internet infrastructure [21,23]. Among the most well-known of China's censorship apparatuses include the Great Firewall, which is the primary technical means of restricting information access at the infrastructure level, which includes blocking undesirable foreign websites such as Facebook and Twitter, regulating access and contents, and monitoring Internet use. But China's censorship infrastructure also extends to include online espionage, regulatory tactics, and social pressure, as MacKinnon, a renowned Internet freedom advocate and former journalist, described:

> Cyber-attacks against activists, dissidents, and Chinese exiles could compromise their computer networks and email accounts. Device and network controls involve pre-installing information filtering and tracking mechanisms in computers and routers sold in China. Domain-name controls prevented ordinary individuals from registering Internet domain names ending in ".cn." Localized disconnection and restriction referred to shutting down connections in specific locations entirely to ensure that locals cannot use the Internet or mobile phones to organize protests. Surveillance works through identity registration for Internet usage, monitoring software, and the compliance of Internet companies. The government proactively steers online

HICSS

conversations through party members, government officials, and "fifty-cent party," people paid to write posts in favor of their employers. [23]

Therefore, not only does the government controls the Internet hardware and software networks, it also imposes a special Internet police force to enforce the government's censorship regulations [21,33].

But the most effective effort at restricting information which emerges at the grassroots level, including chatrooms, microblogs, and online forums, perhaps come not from government's surveillance, but self-censorship of information which organizations and individuals present to their users. Both domestic and foreign Internet corporations such as Google [6] and Yahoo [10] altered their search results to accommodate the state's censorship requirements.

And the Chinese government encourages self-censoring entities to be thorough by intentionally keeping censorship regulations and guidelines generic and ambiguous. Roberts, a scholar studying censorship and propaganda in China, noted:

It is illegal in China to write or distribute any information online that "harms the interest of the nation," "spreads rumors or disturbs social order," "insults or defames third parties," or "jeopardizes the nation's unity." Punishments are similarly ambiguous and unevenly administered—violating online information laws could result in punishment as severe as jail-time to as trivial as having your account shut down or simply removing one offending social media post. The wide range of information that could qualify under these laws keeps online users in China guessing as to what types of information are indeed off-limits and what types of punishment could be meted out for spreading the information. [28]

By providing only highly abstract terms such as national interest, social order, and national unity, the government affords itself more flexibility of interpreting and manipulating legal boundaries [3,21]. Thus, companies which stand to lose much in case of a regulatory misstep tend to deploy sweeping censoring mechanisms to block keywords, ban users, and delete infringing contents [13,21]. The extent of self-censorship may intensify during political events, for example, a case study of keyword blocking on Weibo reported that, during the 2012 National Congress election, Weibo actively manipulated and filtered the search results of certain government officials' names [26]. Even citizens in Hong Kong were worried about the impact of censorship when they engaged in civic activities [19].

But despite popular beliefs, Chinese citizens still maintain a small degree of agency in speaking their minds, as the censorship infrastructure was not designed to completely remove dissents on its Internet. In fact, the Chinese government had investigated citizens' dissents which at times exposed corruption and malfeasance at lower level governments, which contribute to China's effort at cracking down on corrupted officials [8]. Rather, a more important focus for its censorship apparatuses, than to completely eliminate anti-government discourses, are to prevent citizens' collective mobilization and actions. King, et al. examined deleted social media content on the Chinese Internet, arguing that China's censorship is designed to silence comments which encouraged or organized social mobilization; and all forms of mobilization aimed at spurring offline collective actions were targeted regardless of their political inclinations [17]. Thus, Chinese citizens still have limited latitude to conduct political discourses, so long as they could successfully guess at the extent of permissible boundaries.

So far, Chinese citizens' reactions to the Chinese censorship apparatuses have been dialectically complicated. As censorship is continuously strengthened, Chinese are also making use of proxy servers and email to access restricted information [2,22,25]. And citizens have also discussed sensitive topics using substitute terms for blocked keywords [16,24]. For example, "harmony和谐" refers to the ideology of social harmony proposed during Hu Jintao and Wen Jiabao's administration (2003-2013). People use "river crab 河蟹," a homophone of "harmony 和谐," to circumvent the block list of sensitive words [38]. Thus, Roberts suggested that the Chinese censorship not only had not deterred the spread of information, it emboldens Internet users to engage more actively in political writings [28].

3. Related Work

In their seminal work on infrastructure, Star and Ruhleder state that infrastructure is neither a tool or a substrate, but a fundamentally relational concept, which becomes real infrastructure in relation to organized practices [31]. Infrastructure has the following properties: *embeddedness, transparency, reach or scope, learned as part of membership, links with conventions of practice, embodiment of standards, built on an installed base, becomes visible upon breakdown*, and *fixed in modular increments, not all at once or globally* [30]. In many ways, China's censorship shares such properties. It is sunk into and inside of the Internet infrastructure, the organizational arrangements of Internet companies,

technologies, and artifacts as basic as a router. It has reach beyond one single site. It is built upon the existing technical and social structure of the Chinese Internet. It is constructed gradually.

However, China's censorship also differs from the classic conceptualization of infrastructure in important ways. The design of artifacts often contain inscribed values [35]. In this case of censorship in China, it has been deliberately designed and maintained to control and restrict ordinary citizens, rather than to support and enable them in the way that a system of railroad tracks or a city water system function. It is sometimes transparent but other times visible when it functions in intended scenarios. It is learned as people repeatedly encounter and circumvent it. The repressive nature of China's censorship provides us a unique case to reflect upon the understanding of infrastructure.

4. Method

Our study belongs to a larger project investigating how Chinese citizens used digital technologies to understand and discuss political events in China. From April, 2014 to January, 2016, we conducted 32 interviews with mainland Chinese citizens who were active posters of political events in China, and thus were aware of censorship parameters in China and had experience coping with it.

We recruited our interviewees by first identifying Internet sites on which we are likely to find active political posters. We began by registering accounts on Weibo, the largest Chinese micro-blogging service. When a major political event broke out, we used these Weibo's in-site search functions to search related keywords in order to locate online debates and conversations about this event, as well as people involved in these online discourses. And during the period of our investigation, three political events took center stage in these discussions; these include the Umbrella Movement, the National People's Congress, and the crackdown on corruption. The Umbrella Movement was a pro-democracy movement that took place in Hong Kong from September, 2014 to December, 2014. The second event refers to the National People's Congress's annual session that happened in March, 2015. The third refers to the anti-corruption campaign led by Xi Jinping, general secretary of the party, which started in 2012.

We paid particular attention to online celebrities who showed concern for these political events by commenting or re-posting relevant content. These celebrities included scholars, media critics, economists, and journalists. We identified 20 celebrities with the criteria of having one at least post that received over 100 comments. Figure 1 shows an example of a Weibo post with 1341 comments. We viewed each celebrity's micro-blogging page as a site in an ethnographic sense, because each celebrity's population of followers is relatively stable. Additionally, we also observed the same group of people commenting and debating in the comment area. We archived people's conversations from the comment area.

Through the posts of these 20 Weibo celebrities, we identified a pool of interview candidates who had posted multiple meaningful and thoughtful comments. We contacted these people through Weibo's private messaging function to ask for an interview, from which we recruited 32 interviewees. Our 32 interviewees included 19 males and 13 females between the ages of 18 and 46. They had diverse occupations, such as graduate student, government employee, editor, journalist, designer, engineer, programmer, freelancer, and stock manager.

Figure 1. A Weibo Post.

All these interviews were conducted in Chinese. We asked participants how they sought information regarding certain events and whether they experienced censorship during these events. We asked participants about attitudes towards censorship and why they felt as they did. We asked them to describe the situations in which they encountered censorship, and how they coped. We asked how they learned to circumvent censorship. With permission, we followed all the participants' social media accounts. Some of them followed ours in reciprocity. The social media platforms included Weibo, and popular online forums such as tianya.cn and tiexue.net. On these platforms we observed and archived participants' discussion with other social media users.

The first author is a native Chinese speaker. All interviews and social media data were translated into

English by him. We use pseudonyms to protect our participants' identity and anonymity.

5. Data Analysis

We adopted a grounded theory approach [5] to analyze interviews and online discussions. Firstly, we read all interview transcripts and used our initial understanding to produce a starting list of codes, which concern participants' opinions about censorship or their strategies to cope with censorship. From there, we returned to the data to conduct a systematic analysis of the themes that emerged. After several iterations of coding, we identified three concrete methods that our participants used to resist the censorship infrastructure. The three methods are: switching between public and private channels, using machine unreadable message, and broadening information search. We then returned to our data set to find episodes [29] where participants described their strategies of resistance. We paid particular attention to their reasoning processes behind adopting a particular strategy.

6. Findings

In this section, we detailed participants' strategies to navigate information allowed by censorship on the Chinese Internet. One, participants have used alternative backchannels. Two, they have presented information in creative ways. And three, they have pieced together information from multiple, local and foreign, sources to reassemble the complete picture.

6.1. Reserving Sensitive Information for Private and Backchannel Discussion

Most of our participants, from their experiences navigating the Chinese Internet, have perceived that the use of government censorship apparatuses is more evident on popular websites, as well as many-to-many public channels (e.g., Weibo). Their experiences with government censorship usually involved uninformed and sudden manipulation of public information, such as: they were suddenly unable to visit a particular news website; they could not enter a previously admissible keyword search term into a search field; they found particular content on social media to be deleted; and they saw suspicious comments which they believed were posted by paid commentators hired by the government. Through such in-situ experiences, Chinese Internet users observed and guessed at what

is permissible by censorship, and learned what they should not say publicly. They kept this sensitive information off the public record and only to be shared through private backchannels, such as in instant messaging and private chats. For example, Ling, a magazine editor, said:

> I think the government only banned keywords in places where a lot of people can read and talk. When I used blogging services a while ago, I had to make sure there was no sensitive word in my articles each containing hundreds of words. However, I have never had to worry about this problem [word checking] when chatting in a private channel.

QQ and WeChat are the most popular instant messaging tools in China [4]. Tianya.cn is one of the largest online forum. And Mingyue, a graduate student, said:

> They [the government and the owners of social media platforms] don't really care about what we say in instant messaging tools such as QQ and WeChat, or private chat on Weibo and tianya.cn.

While the extent of Internet information which the Chinese government intends to censor remains unclear, Chinese users tended to believe censorship does not apply to private chat channels, as Zhongfeng, a 27-year-old designer, told us:

> It's very hard to monitor all the private communication. There will be too much content to censor. Also in private chat we don't type in formal Chinese, which makes censorship even harder to work.

Under the pervasive surveillance, our participants generally perceived private channels to contain more reliable information than public channels, which tended to be generic and shallow. Thus, serious information seekers had often directly asked for information from people who they believed had sensitive information. For example, Baozi, a 20-year-old college student, mentioned that he had friends who studied at Hong Kong during the period of the Umbrella Movement. He could often see his friends' social media posts about the movement, such as pictures or related news report. He told us:

> Yeah, I initially learned about the movement from my friends' posts in WeChat's Friend Circle. But they didn't really post many details of the movement, except a few pictures and very brief comments. Maybe it is kind of sensitive to talk in the public. For example, if I asked a question in their posts' comment area, most likely they would answer briefly with some joking language. But I got really interested in this and chatted with them privately, they began to talk a lot about their experiences with the movement, such as class

boycott activities and protesting in Hong Kong's business district.

Baozi found private channels to be more effective at obtaining information from his friends; he thus resorted to private channels in order to obtain a better picture.

Our participants reported that in some social media circles, such as on Weibo, users were mostly willing to share information privately, even with strangers, so long as this happened away from public eye. Zhongfeng described this open mindset regarding Weibo information sharing:

> In Weibo discussions, I often come across novel and insightful ideas that I have never heard before. Some of the ideas refer to sensitive information, such as the relationship between Hong Kong's capitalists and high-ranking central government officials. There will never be reports like this in the domestic media because of censorship. If I am interested in that piece of sensitive information, I will send a private message to the user and ask for it. Most of the time, the user is willing to share it. I do the same thing if I have certain sensitive information and another person asks for it.

Zhongfeng's story signified how Chinese Internet practices changed to develop new informational pathways (i.e., a network of private backchannels) which can partially counter the influence of the censorship infrastructure. This backchannel replaced normative participation in Habermas' sense of public sphere [7,11], and traversed a longer and secured route perceived as off the censorship radar. We are unable to know the extent this information "rerouting" diminishes public discourses, but what is interesting is the emergence of consensus among Weibo users making such forms of information sharing plausible. Private and backchannel discussions signified how Chinese citizens came to understand the boundaries of Internet censorship and figure out the venues that the censorship infrastructure does not reach.

6.2. Expressing in Machine Unreadable Ways

A common perception among our participants was that many censorship mechanisms relied on basic keyword filtering techniques to manage the massive, ever-increasing amount of information that was being produced and circulated in the Chinese Internet. To counter this mechanism, participants attempted to make communications difficult to read or delete by either algorithms or human. For example, Zhongfeng believed that censorship mechanisms typically followed a set of simplistic reasoning, such as to identify a set of sensitive keywords:

> [The government's] methods are relatively brutal, such as enforcing the sensitive word list. But you know, who really talk in formal language online?

What Zhongfeng pointed out was also reported in previous studies on how Chinese users were able to use uncensored terms to express the same politicized meanings without being censored [27,34,37]. What is important here is that the Chinese users have evolved their Internet expressions in ways faster than censorship could keep up.

One way which participants could bypass censorship was to render text as bitmaps, a form of content which current censorship mechanisms could not read (see Figure 2).

Figure 2. Image-based Content.

Yuming, a 23-year-old college student, enjoyed using images for opinion expression. He said:

> I absolutely love it. I can say something that would be deleted otherwise. I can also be more expressive with images, like using some interesting fonts or adding some Internet meme pictures.

While it took effort to produce such images, participants found them useful when they deemed the content sensitive.

The second way was to post sensitive information only on temporary "throwaway" accounts [20]. While censorship could pick up accounts which have been posting sensitive information, and ban these accounts, it has yet to be able to trace the identity of the real user—if such person manages to move from one account to another. Here is an excerpt of a social media conversation:

Feitu: You are very knowledgeable. I will have to admit that I know little about the movement. Can you send some information to me through private messages if it is convenient for you? I want to know more.

Wuhui: You should follow a Weibo account titled *huaxia* ("华夏"). This person often publishes precise analysis, and I believe he knows a lot of sensitive information. However, Weibo often bans his account, probably because he leaks too much information. To counter account suspension from Weibo, he has created a primary Weibo account that regularly publishes his newly registered accounts. Once you have followed this account, he will tell you the name of his primary account in private messages. If you can follow his primary account, you will always know his latest Weibo account for leaking sensitive information.

In this conversation, Wuhui talked about a successful approach employed by *huaxia* in which his master account was used to publish the usernames of throwaway accounts; and these throwaway accounts were used to publish sensitive information. His master account had never been banned since it did not directly post this information. Such approach outwitted the current censoring mechanism and allowed the audience to continue to receive sensitive information.

The third way was to obtain information from lesser known websites. Participants pointed out that many websites which have been aggregating news from blocked foreign websites had published materials without the government knowledge. For example, qimila.com was a Chinese video sharing forum where people shared downloaded news videos from blocked foreign websites such as YouTube. These videos often involved sensitive topics in China. Another powerful website was *Long Teng Wang* ("龙腾网") (www.ltaaa.com/), where Chinese citizens voluntarily translated and shared many countries' reports about China, Hong Kong, and Taiwan. Leiyu, a 21-year-old college student, highlighted the value of these aggregation websites:

I often use a number of channels to obtain information. For example, search *Long Teng Wang* on the Internet. This is a translation forum... I know many powerful websites like this. Therefore, I do not rely on Weibo for information.

Leiyu's story signified the existence of alternative websites that allowed the access to rich content unseen in mainstream media sites, although in a much more complex way.

6.3. Piecing the Puzzle Through Broad-based Information Search

Despite having ways to circumvent and bypass censorship, our participants still found value in consuming censored information, especially if each piece of information contributes to forming the complete story. And our participants judged the value of censored information in the following ways.

One, if the reported event was of little political value, its related news was likely to be accurate, as a participant said:

For events with lower priority, I am fine with just reading the state media. I do not necessarily trust what the state media says.

Two, even for strictly censored content on state media, our participants had found it useful to deduce the premise of that information being reported—by drawing on the circumstances in which the information is being presented. For example, Gushi, a 46-year-old stock manager, said:

I watch Xinwen Lianbo every day to inform my investment decisions. I try to infer which industry the central government favors.

Three, when our participants read local censored news from different outlets, they could also identify subtle differences which complemented what each outlet had de-emphasized. And Mafei, a 29-year-old engineer, enjoyed reading a number of mainland-based newspapers on a weekly basis. Due to China enforcing vague self-censorship regulations, each media outlet might interpret what is considered sensitive information differently. And he found a variety of competing opinions even on these media. He also considered social media such as Weibo and WeChat as complementary to state media.

Finally, our participants looked beyond each information source by reading broadly, while piecing together different information to form a coherent picture. Some of them even gathered information from foreign sources, so as to form a more complete picture of social and political events. For example, Zhelu, a 37-year-old writer, watched state-owned television channels for daily entertainment and news. But he was also a 15-year customer of several Hong Kong television channels because of their alternative analyses of international and domestic affairs. He also logged on to Facebook and Twitter, via VPN, to learn about his Western friends' opinions. While acknowledging the quality of information they obtained from Western sources, our participants also stressed that even foreign-based and Western news media have their biases, as Leiyu commented:

Knowing each media's pros and cons and taking advantage of this knowledge is necessary to

understanding what's really going on in an event. In the end, if you do enough homework, censorship won't matter much.

By developing a rich understanding of each media's pros and cons, our participants developed their own taxonomies of media outlets—with their complementary biases and perspectives—in order to piece the puzzles of political biases on the Internet. Participants were confident that censorship could not stop them from obtaining desired information.

7. Discussion

We reported a qualitative study of a group of Chinese citizens' practices of resisting censorship that is pervasive in the Chinese Internet. Our participants utilized many different strategies at circumventing, outwitting, and looking beyond censored information. For example, they learned what information was best conveyed in private instant messaging, rather than an online forum. Some Weibo users even developed trust with each other in relaying information through private messaging. Other such social practices include the use of non-machine readable images and news aggregate with deductive reasoning. Through these social practices, the citizens were able to broaden their information accessibility beyond what is prescribed by censorship. Next we will discuss how this case study might advance our understanding of the censorship infrastructure as well as infrastructural resistance.

7.1. Characterizing Repressive Infrastructure

Previous studies have primarily examined infrastructures designed to enable people and serve society [1,12,31]. China's censorship presents a unique case where a sophisticated system has been built and maintained at a national scale with the sole purpose of controlling and limiting every ordinary citizen.

The censorship infrastructure possesses a few unique characteristics. First, its goal is to set boundaries, rather than to support and to empower. In order to do so, the censorship infrastructure operates in a top-down manner. The central government sends out orders and decisions while corporations and government agencies execute these instructions.

Second, it becomes visible whenever people cross the boundaries, such as searching a sensitive keyword or visiting a blocked site.

Third, the censorship infrastructure is meant to be opaque. No ordinary citizen should know its standards and mechanism. Our participants might

observe a blocked foreign website or a forbidden search engine keyword. However, they would never know the precise list of blocked websites or the sensitive keyword list. Remaining an opaque artifact, the infrastructure could easily extend its influence beyond its reach, since participants could not be completely certain whether they were being watched. Internet companies are likely to censor more than they have to in order to limit their exposure to regulatory infringements.

The well-known existence of such a massive repressive infrastructure might be possible in centralized regimes that are able to execute top-down methods of control, with the compliance of companies and organizations. However, repressive infrastructures might exist at varied scales in different societies, only becoming visible when they malfunction in an unexpected way, as evidenced by the Snowden case and NSA's massive surveillance effort [9]. Additionally, there might be a repressive side of our everyday infrastructures. Such concern increases when infrastructures fall into private hands that are not subject to public eyes. The infrastructure that ordinary citizens rely on for information and news consumption is worth research attention [18]. For example, Internet companies such as Google, Twitter, and Facebook are gaining enormous power in today's internet infrastructure, as a substantial portion of the Internet traffic flows through these Internet giants' sites [36]. Google, for example, has been frequently cited for its discriminating algorithms [14,15]. Facebook was reported to manipulate its trending topics to favor the Democratic Party in the US [32].

Studying repressive infrastructure can be challenging. In this study, there has been no open, official documentation regarding how censorship is implemented and maintained, what entities participate, and what technologies are designed and utilized. Therefore, we were hardly able to follow Star's recommendations [30] to identify master narratives or surface invisible work. Instead, we analyzed people's encounters and experiences with censorship, as well as their interpretations of how censorship worked. The secretive nature of such infrastructure and the proper approach to it are worth further investigation by infrastructure researchers.

7.2. Understanding Infrastructural Resistance

Much learning took place as Chinese citizens became used to the pervasiveness of censorship. They had to learn the advantages and disadvantages

of different venues. Because of the opaqueness of censorship, participants mostly built knowledge through incidental observations of censorship as well as chatting with other citizens.

Participants' infrastructural resistance involved three parties—*companies* developing authoritative mechanisms with over-reaching censorship, the *censorship authority* imposing vague censorship regulations with hidden boundaries, and *citizens* performing resistance by pushing informational boundaries presented. The nature of this resistance is not to disregard the entirety of government's censorship, but to navigate the gray areas between "censored information" and the "level of information (actually) permissible by censorship." Citizens make use of social media to access and transmit information beyond what was permissible by censorship. Yet, information that has been shared by overriding intents and designs of censorship may not have exceeded what the government intend on suppressing. As discussed by Roberts [28], and also mentioned by our participants, the extent of Chinese government censorship may be aimed at disallowing public gatherings and collective actions, and perhaps for this reason, the censorship apparatuses had not been extended to less popular websites and instant messaging tools.

Participants' infrastructural resistance was a collaborative effort that involved both friends and strangers. Participants had friends who located outside the censorship infrastructure and had easy access to sensitive information. They also felt free to ask strangers for information. Participants were confident that, as long as they have access to the Internet, they will be able to find any desired information by collaborating and communicating with other people. We attribute such confidence to the ubiquitous Internet infrastructure that is composed of various ways of communication and massive numbers of organizations and people. Embedded in the Internet infrastructure, repressive infrastructures do not have absolute control over information and resistance is possible.

8. Conclusion

In this paper we reported a qualitative study of a group of Chinese citizens coping with China's Internet censorship infrastructure. By analyzing participants' three concrete strategies to navigate the censored Chinese Internet, we were not stating that such strategies were common and usual among our participants. Moreover, we do not see repression as the only characteristic of China's censorship. Rather,

the paper is intended to explore the relationship between resistance, repression, and infrastructure, without either supporting or denouncing censorship. We showed how a repressive censorship infrastructure worked as participants experienced it, as well as how infrastructural resistance was possible through individual agency and social collaboration.

9. Acknowledgements

10. References

[1] Borgman, C.L. *Scholarship in the Digital Age: Information, Infrastructure, and the Internet*. The MIT Press, 2010.

[2] Cherry, S. The net effect: as China's Internet gets a much-needed makeover, will the new network promote freedom or curtail it? *IEEE Spectrum 42*, 6 (2005), 38–44.

[3] Cheung, A.S.Y. The Business of Governance: China's Legislation on Content Regulation in Cyberspace. *International Law and Politics 38*, (2006), 1–37.

[4] CIW Team. Tencent in Q3 2015: QQ MAUs 850M, WeChat MAUs 650M. *China Internet Watch*, 2015. http://www.chinainternetwatch.com/15592/tencent-q3-2015/.

[5] Corbin, J. and Strauss, A. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, 2007.

[6] Cunningham, A. Report: Google will comply with censorship laws to get Play into China. *arstechnica*, 2015. http://arstechnica.com/gadgets/2015/09/report-google-will-comply-with-censorship-laws-to-get-play-into-china/.

[7] Dahlgren, P. In Search of the Talkative Public: Media, Deliberative Democracy and Civic Culture. *Javnost - The Public 9*, 3 (2002).

[8] Givens, J.W. and MacDonald, A.W. The Internet with Chinese Characteristics: Democratizing Discourse But Not Politics. *APSA 2013 Annual Meeting*, (2013), 19.

[9] Greenwald, G. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Henry Holt and Company, 2014.

[10] Gunther, M. Tech execs get grilled over China business. *CNN*, 2006. http://money.cnn.com/2006/02/15/news/international/pluggedin_fortune/index.htm?cnn=yes.

[11] Habermas, J. *The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*. MIT Press, 1991.

[12] Hanseth, O., Monteiro, E., and Hatling, M. Developing Information Infrastructure: The Tension Between Standardization and Flexibility. *Science, Technology & Human Values 21*, 4 (1996), 407–426.

[13] Human Rights Watch. China: Nationwide Arrests of

Activists, Critics Multiply. *Human Rights Watch*, 2013. http://www.hrw.org/news/2013/08/30/china-nationwide-arrests-activists-critics-multiply.

[14] Introna, L. and Nissenbaum, H. Shaping the Web: Why the Politics of Search Engines Matters. *The Information Society 16*, 3 (2000), 169–185.

[15] Introna, L.D. Maintaining the reversibility of foldings: Making the ethics (politics) of information technology visible. *Ethics and Information Technology 9*, 1 (2006), 11–25.

[16] Jiang, M. The Co-Evolution of the Internet, (Un)Civil Society & Authoritarianism in China. In *The Internet, Social Media, and a Changing China*. University of Pennsylvania Press, Philadelphia, PA, 2014.

[17] King, G., Pan, J., and Roberts, M. How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review 107*, 2 (2013), 326–343.

[18] Kou, Y. and Nardi, B. Rethinking Civic Computing in China. *First Monday 21*, 7 (2016).

[19] Kow, Y.M., Kou, Y., Semaan, B., and Cheng, W. Mediating the Undercurrents: Using Social Media to Sustain a Social Movement. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, ACM Press (2016), 3883–3894.

[20] Leavitt, A. "This is a Throwaway Account": Temporary Technical Identities and Perceptions of Anonymity in a Massive Online Community. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15*, ACM Press (2015), 317–327.

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

[22] MacKinnon, R. Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice 134*, 1–2 (2007), 31–46.

[23] MacKinnon, R. China's "Networked Authoritarianism." *Journal of Democracy 22*, 2011, 32–46.

[24] Mina, A.X. Batman, Pandaman and the Blind Man: A Case Study in Social Change Memes and Internet Censorship in China. *Journal of Visual Culture 13*, 3 (2014), 359–375.

[25] Nardi, B. Virtuality. *Annual Review of Anthropology 44*, 1 (2015).

[26] Ng, J.Q. and Landry, P.F. The Political Hierarchy of Censorship: An Analysis of Keyword Blocking of CCP Officials' Names on Sina Weibo Before and After the 2012 National Congress (S)election. (2013).

[27] Rauchfleisch, A. and Schäfer, M.S. Multiple public spheres of Weibo: a typology of forms and potentials of online public spheres in China. *Information, Communication & Society*, (2014), 1–17.

[28] Roberts, M. *Experiencing Censorship Emboldens Internet Users and Decreases Government Support in China*. 2015.

[29] Schwandt, T.A. Qualitative data analysis: An expanded sourcebook. *Evaluation and Program Planning 19*, 1996, 106–107.

[30] Star, S.L. The Ethnography of Infrastructure. *American Behavioral Scientist 43*, 3 (1999), 377–391.

[31] Star, S.L. and Ruhleder, K. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research 7*, 1 (1996), 111–134.

[32] Statt, N. Facebook denies systemic bias in Trending Topics but changes how they are chosen. *The Verge*, 2016. http://www.theverge.com/2016/5/23/11754812/facebook-trending-topics-changes-political-bias-senate-inquiry.

[33] Tsui, L. The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China. *China Information 17*, 2 (2003), 65–82.

[34] Wang, D. and Mark, G. Internet Censorship in China: Examining User Awareness and Attitudes. *ACM Transactions on Computer-Human Interaction 22*, 6 (2015), 1–22.

[35] Winner, L. Do Artifacts Have Politics? *Modern Technology: Problem or Opportunity 109*, 1 (1980), 121–136.

[36] Worstall, T. Fascinating Number: Google Is Now 40% Of The Internet. *Forbes*, 2013. http://www.forbes.com/sites/timworstall/2013/08/17/fascinating-number-google-is-now-40-of-the-internet/#2192080b6ca2.

[37] Yang, G. *The Power of the Internet in China: Citizen Activism Online*. Columbia University Press, 2013.

[38] Yang, G. and Jiang, M. The networked practice of online political satire in China: Between ritual and resistance. *International Communication Gazette 77*, 3 (2015), 215–231.