GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

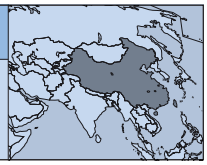
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

CHINA

Discourse deferred: PRC netizens swap public microblogs for the not-so-private digital dinner table



Danwei
Hudson Lockett
Danwei.com

Introduction

Before the internet, complaints about sensitive issues in mainland China were confined largely to small private gatherings – often around the dinner table, away from prying cadres' ears. Today, to better understand the role that online surveillance may now play in the People's Republic of China (PRC), it must be analysed in the context of a broader information control apparatus and the mainland's unique social media environment.

With foreign social media platforms like Twitter blocked on the mainland, homegrown microblogs, or weibo (微博), finally came into their own in the early 2010s as a *de facto* public sphere. The rapid spread of information on Sina Corp's Weibo (新浪微博) microblog platform concerning the 2011 Wenzhou high-speed rail crash (see GISWatch 2011),[1] together with its subsequent role in the scandal leading to the ouster of top leadership candidate Bo Xilai (see GISWatch 2012),[2] drove that point further home for the ruling Chinese Communist Party (CCP). Even Sina's in-company censorship efforts seemed unable to quiet the beast it had birthed.

Two new actors have since swung a pair of sledgehammers to the knees of mainland microblogs, forever changing the country's online ecosystem. The first is the popular app WeChat (branded locally in Mandarin as Weixin 微信, or "micro-message") developed by Tencent Holdings Limited. WeChat began as a smartphone instant-messaging service, but soon evolved into a versatile private social networking platform and communications tool whose functions even included limited public microblogging. By the end of 2013 it had unseated Sina's Weibo as the social networking platform of choice.

The second actor is current CCP General Secretary and PRC President Xi Jinping, who was elevated to the former office in November 2012, and assumed the latter as a matter of course in March 2013. Xi wasted little time in launching a renewed crackdown on dissent – a key front of which was the unruly and critical online chatter that his predecessors had left unquashed. He would confront it with gusto.

Background

Surveillance of the internet's Chinese-language public face has become increasingly sophisticated as the CCP has sought to use it both as a means to keep tabs on public opinion and a tool to monitor and control speech. Officials are typically mum on the more Orwellian aspects of this effort, but local, privately owned companies such as XD Tech (线点科技) openly offer mass surveillance, analysis and keyword alert services to both central and local governments. XD Tech, which opened for business in Beijing in 2005, lists two of the most important party organs among its clients: the General Office of the CCP's Central Committee, and the powerful and secretive Central Organisation Department responsible for choosing where Party officials are posted for every step in their careers. Other major clients include the Public Security Department of Guangdong Province, state-owned Bank of China and all three mainland telecom operators (also state-owned).

However, survey results published in March 2014 commissioned by the BBC World Service showed that 76% of Chinese respondents said they felt free from government monitoring – the highest proportion of any country polled.[3] Unlike censorship, the surveillance of private information, especially when stored server-side rather than on user devices, can be difficult to verify.[4] Evidence of government surveillance of WeChat and other such private communication platforms was previously

1 www.giswatch.org/en/country-report/civil-society-participation/china

2 www.giswatch.org/en/country-report/internet-and-corruption/china

3 Globescan. (2014, March 31). One-in-Two Say Internet Unsafe Place for Expressing Views: Global Poll. *Globescan*. www.globescan.com/news-and-analysis/press-releases/press-releases-2014/307-one-in-two-say-internet-unsafe-place-for-expressing-views-global-poll.html

4 The Citizen Lab. (2013). *Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*. https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications

harder to come by. But a few days before Xi Jinping's ascent to CCP leadership in late 2012, dissident Hu Jia posted on Twitter (translated):

> Tencent-developed "WeChat" is extraordinarily popular on the mainland. Domestic Security Police use it to investigate communications between mainland dissidents. The voice messages, text and pictures we use WeChat to send all go directly into Domestic Security's technical investigation system, and are just as easily monitored as phone calls and text messages.

That week Hu Jia told the *South China Morning Post* that he had long expected his phone calls and text messages to be tapped by state-owned telecom providers, but previously assumed that WeChat was not compromised. Now he claimed Domestic Security officers had recited, word for word, private voice-message exchanges between him and his friends shortly after they had occurred on WeChat. He said friends had also been interrogated about WeChat conversations that took place only an hour earlier, and gave an example of Domestic Security officers using information from voice messages to track him in real time when he and a friend tried to change a meeting's venue at the last minute.

Part 1: Twilight of the microblogs (2013)

Once Xi became general secretary his administration wasted little time in launching vigorous crackdowns on both official corruption and dissent. The two drives conflicted when a group called the New Citizens' Movement pushed for officials to declare their assets and follow rule of law as outlined in the PRC's constitution. These calls, online and off, were silenced, and the group's leaders detained or arrested and brought to trial under various pretexts.

That August, one year since WeChat's user base had surpassed Sina Weibo's, Tencent added microblog-like "public" accounts to its now flagship service/software. Standard private accounts were still limited in how many people could join a given "friend circle" (100, as of this writing), but all users could now follow unlimited *public* accounts, each of which could send one message a day to all subscribers.

Then, on 10 September, the Supreme People's Court and the Supreme People's Procuratorate issued a landmark joint interpretation of PRC criminal law that gave further firepower to censorship efforts: authors of any Weibo or WeChat posts that had been "re-tweeted" 500 times or viewed 5,000 times would be legally liable for any misinformation or illicit content authorities found therein. While such rulings are not binding precedents that determine subsequent court decisions in the PRC, the message was clear: posts containing unsanctioned information or opinions could result in real punishment.

In fact, a name-and-shame campaign targeting Sina Weibo's most influential verified users ("Big Vs") was already underway. In late August, Chinese-American angel investor and Weibo heavyweight Charles Xue was arrested in Beijing on charges of soliciting a prostitute. But in an on-air confession broadcast nationwide, a handcuffed Xue spoke only of his regret over abusing his power to spread misinformation and rumours among his 12 million followers. This intensified crackdown added momentum to already powerful market forces: Weibo activity further waned as WeChat's moon waxed gibbous.

Critical online discourse went to ground at the apparently more private WeChat, but the October arrest of venture capitalist Wang Gongquan, a backer of the New Citizens Movement, soon called the platform's privacy into question. When Sina shuttered his Weibo account with 1.5 million followers in 2012, Wang shifted to a standard WeChat account to continue his activism. However, the more private nature of this venue did not stop authorities from detaining and then formally arresting Wang the following year on charges of disturbing public order.

A report by the Public Opinion Monitoring Centre of the state-run *People's Daily* announced on 30 October that the campaign against Big V's had succeeded – the government had retaken online space for the Party. The state-run *Beijing Youth Daily* capped the year off on 13 November by claiming Sina had taken action against 103,673 accounts for flouting online behaviour guidelines announced that summer, through measures ranging from temporarily restricting users' ability to post to permanent account deletion.

Part 2: Dawn of the digital dinner table (2014)

After a few months' lull, Xinhua reported on 27 February that Xi Jinping was now heading "a central internet security and informatisation leading group" and had that day presided over its first meeting. (Xi has become the leader of other such internal leadership committees since his ascent, and has established other new ones for policy change and domestic security.) A same-day report on CCTV said Xi had emphasised the need for a firm hold on the guidance of public opinion online.

Then on 13 March, WeChat saw its first real purge: Tencent deleted at least 40 critical public

accounts, some with hundreds of thousands of subscribers. On 15 March, the *South China Morning Post* reported that according to an unnamed industry source, a team of government censors were stationed at Tencent's Guangzhou office for a week before the crackdown; censors instructed the company to practice self-censorship on accounts posting "sensitive content on national politics", and named certain accounts that had to be shuttered.

But as March dragged on a major labour dispute in Southern China would provide contrasting examples of WeChat's potential in both grassroots organising and surveillance. Tens of thousands of workers for shoe manufacturer Yue Yuen used WeChat to coordinate a crippling strike in Guangdong without help from their sanctioned, government-run provincial union; meanwhile police detained labour advocate Lin Dong from the Shenzhen Chunfeng Labour Dispute Service Centre on the grounds that he had posted inaccurate information online. The centre's director Zhang Zhiru told the *South China Morning Post* that Lin had only sent a private WeChat group message to 11 people about the issue, and had noted the information was unverified. While the strike was ultimately successful and Lin was released after 30 days in custody, the biggest guns were still waiting in the wings.

On the morning of 27 May authorities announced a social media crackdown one week before the 25th anniversary of the 4 June massacre that ended the Tiananmen Square protests.The special month-long operation specifically targeting WeChat and similar apps would be carried out by major government organs including the State Internet Information Office, the Ministry of Industry and Information Technology, and the Ministry of Public Security. Their stated focus was on public accounts with social mobilisation power. Less attention was given to a new development in how Tencent would approach the social feature that had long been one of WeChat's central conceits: private friend circles.

After WeChat was explicitly named at the crackdown's outset, Tencent and six competitors quickly published a list of 10 proposed industry "initiatives" to help create a "clean internet"; these included a new commitment to further scrutinise private groups. The companies called on industry peers to "intensify management of friend circles and regulate related functions, intensify the inspection and management of friend circles' content, and resolutely shut down accounts that transmit illegal and harmful information via friend circles."

Tencent then announced on 10 June that during the year's first six months it had already shuttered 20 million private WeChat accounts with the help of authorities, in addition to 30,000 public accounts it had deemed fraudulent. In announcing the move, dubbed "Operation Thunder", Tencent claimed the accounts had been guilty of engaging in phishing schemes or prostitution. That day it also announced that the search engine Sogou (搜狗) of the eponymous company it had acquired last year was now capable of searching public WeChat accounts, allowing users to look them up and browse their posts' contents.

Almost as an afterthought the campaign turned its eyes to Apple: the Ministry of Industry and Information Technology announced it would take new measures to regulate the company's iMessage service. A group chat function similar to WeChat's friend circles was added to the Apple instant-messaging app in October 2011; Chinese tech industry news site *Techweb* reported the new measures would include tools to monitor and prevent spam messages, which it claimed had cost users millions of RMB. Finally, following a pro-democracy march in Hong Kong on 1 July that drew a historic turnout of hundreds of thousands according to organisers, messaging apps Line and KaoKao Talk began experiencing issues, with the former rendered completely inaccessible.

Conclusions

Survey results indicate a widespread belief that surveillance on the mainland does not affect or bother with most people's affairs. Until recently even experienced dissidents believed themselves free from snooping eyes and ears on WeChat. Hu and Wang's cases show us that assumptions about what is private online in the PRC do not always hold true, particularly when one uses a supposedly private space to organise. In mainland China the internet and everything in it can reasonably be viewed as public space – that is, ultimately belonging to the state.

Operation of online communications platforms by private companies is a privilege, not a right. The threat of its rescindment will compel corporations to comply with state demands lest they lose permission to stay online. Sina's failure to effectively clamp down on recusant expression eventually prompted more severe government action, though user migration to WeChat was already well underway before this. By more promptly complying with government directives and effectively dealing preemptively with areas of potential concern, Tencent may be able to keep WeChat from coming to the same grisly end.

Much still depends on how netizens take advantage of WeChat's many functions. The massive March strike in Guangdong shows that even friend circles limited to 100 members can spread information rapidly enough between overlapping groups to mobilise tens of thousands, while labour advocate Lin Dong's detainment shows that even very small-scale group communication can serve as a pretext for detention if one helps effectively focus and direct the momentum of such large-scale movements. But even Tencent's in-company surveillance and control efforts may not be as all-powerful as the past year seems to imply. In light of how private PRC companies already provide surveillance services individually to different sectors of the government and Party, the publicly projected monolithic censorship and surveillance effort of Xi's administration may belie an unseen and far more piecemeal approach.

For now, though, critical conversations online have taken refuge in a space that those around before the internet may find familiar: a sort of a digital dinner table, albeit one where conversations are much more easily listened in on. Complaints will continue in semi-private, but this suits the CCP just fine: where before all eyes were struggling to follow a flurry of public microblogs, now only the party has potential access to a comprehensive view of online discourse that could ultimately strengthen its hold on power. While it may not be able to fully stamp out dissent, neither does the party seem likely to face a Snowden of its own any time soon.

Of course, few saw the fall of Bo Xilai coming, either – aside perhaps from Bo's former right-hand man Wang Lijun, who fled to the closest US consulate when he feared his old boss might have him killed, a stack of classified documents in hand for use as a bargaining chip (see again GISWatch 2012).

Action steps

The following action steps can be suggested for China:

- The same basic precautions recommended against National Security Agency (NSA) surveillance all hold true in the PRC: cryptographic anonymity tools are necessary for true privacy in communication. However, unlike in the US, public debate and opposition to the state's surveillance of its own citizens appears impossible without broader public consciousness of these endeavours and systemic political changes.
- Applications and online services made by PRC companies whose servers are on the mainland can be considered to be at least potentially compromised.
- Mobile communication seems particularly vulnerable to surveillance, and likely cannot be relied on for anonymity; this is doubly true if a user is a dissident or known member of advocacy or activist groups that serve organisational purposes.
- While not touched on above, foreign news organisations and businesses are often subject to state-directed hacking efforts in the PRC. WeChat and other such local networking apps, while convenient, essentially create a detailed record of user activity and contacts that can help undermine other efforts to maintain privacy and confidentiality.