

2011

## Review: *Consent of the Networked*

Anne Henochowicz  
*China Digital Times*

Follow this and additional works at: <http://digitalcommons.unl.edu/chinabeatarchive>

 Part of the [Asian History Commons](#), [Asian Studies Commons](#), [Chinese Studies Commons](#), and the [International Relations Commons](#)

---

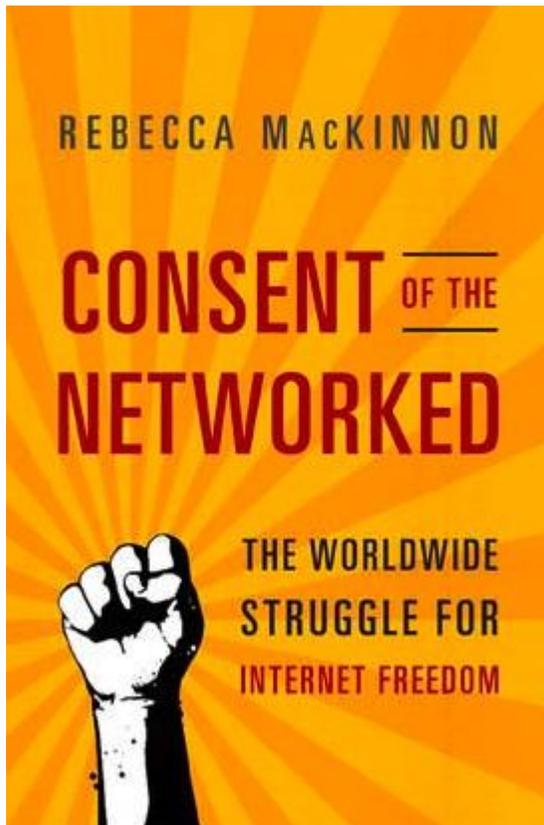
Henochowicz, Anne, "Review: *Consent of the Networked*" (2011). *The China Beat Blog Archive 2008-2012*. 17.  
<http://digitalcommons.unl.edu/chinabeatarchive/17>

This Article is brought to you for free and open access by the China Beat Archive at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in The China Beat Blog Archive 2008-2012 by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

## [Review: \*Consent of the Networked\*](#)

April 17, 2012 in [Books](#) by [The China Beat](#)

By Anne Henochowicz



The last two years have seen much talk about the explosion of social media as a tool of real change, most notably during the Arab Spring. Tunisia's and Egypt's revolutions were powered by Twitter and Facebook. Though these sites are blocked in China, Sina's microblogging platform Weibo has also changed the political game in that country, forcing government accountability after last summer's high-speed train crash in Wenzhou and contributing to the very public downfall of former Chongqing Party Secretary Bo Xilai. Weibo's power may also lead to its demise. After rumors of a coup attempt spread recently, [the comment function on posts was disabled from March 31 through April 3](#).

The rise of Weibo, concurrent with a tightening of restrictions on activists, has focused the world's attention on Chinese social media. The cat-and-mouse game Chinese "netizens" play with the censors has made it onto the pages of the [New York Times](#), [The Economist](#), and the [International Herald Tribune](#). What is so often missing, though, from the discussion of Internet freedom in China, as in the Middle East, is the role that "free world" business and politics plays in the mechanisms of censorship.

Rebecca MacKinnon's [Consent of the Networked](#) is a synthesis of the global debate over Internet freedom. MacKinnon has extensive journalistic experience in China, but her book encompasses

the breadth of Internet issues worldwide. The CNN Beijing bureau chief from 1998-2001, MacKinnon went on to become a fellow at Harvard's Kennedy School of Government, and later the Berkman Center for Internet and Society. She is the co-founder of Global Voices, an international citizen journalist blog. She is currently a fellow at the New America Foundation and on the Global Network Initiative's board of directors.

MacKinnon argues that Internet freedom depends on the "consent of the networked." Like John Locke's consent of the governed, the denizens of the Internet, its "netizens," relinquish a certain amount of personal freedom in exchange for security. In the physical world, we accept that we need the police to protect us from harm. If the police are too weak, we don't feel safe in public. But if the police have too much power, they bring a new kind of danger into our lives. Like real-world institutions, our virtual hegemony should guarantee our freedoms, not encroach on them.

The trouble with the Internet is that the kingdoms governing it—Facebook, Google, Yahoo—make their own rules. They are not accountable to netizens. They may apply their laws arbitrarily or change them without warning. Facebook, for example, has a loosely-enforced real-name policy. Zhao Jing, the Beijing blogger and journalist who goes by the pen name Michael Anti, found his Facebook account shuttered in 2011 for violation of the company's real-name policy. But the same policy has not been applied to Beast, Facebook CEO Mark Zuckerberg's dog.

Zuckerberg argues that netizens should have nothing to hide online. But control over how much personal information exists about us online is vital to our real-world safety, whether we inhabit democracies or authoritarian regimes. Under South Korea's short-lived real-identification registration requirement, netizens' identities on the blogging platform Daum, YouTube, and other sites were tied to real names, ID numbers, and addresses. This allowed for the 2009 arrest of Park Dae-sung for "spreading false information to harm the public interest," even though he blogged under a pseudonym. The real-name regulations remained until July 2011, when the national ID numbers of about 35 million people were stolen from a popular Korean Web portal.

China's four biggest microblogging platforms, including Sina Weibo, are phasing in real-ID requirements as of March 16. Users can keep their unregistered accounts, but eventually will not be able to post without giving their real names and mobile phone numbers. This not only threatens Weibo's freewheeling atmosphere, but also leaves users vulnerable to identity theft.

It is easy to pin all of the blame on the Chinese government. Twitter, Facebook, YouTube and Google all had their time in China, before some "mass incident" or conflict between the company and the government threw it on the other side of the Great Firewall. But we should not forget that American Internet and technology companies have also played a role in online censorship. Perhaps the most egregious example is the case of journalist Shi Tao, arrested in 2004 after sending an email from his Yahoo account to the organization Democracy Forum about directives for reporters leading up to June 4. At the Beijing state security bureau's request, Yahoo turned in all of Shi's "login times, corresponding IP addresses, and relevant email content." Shi is still serving his jail sentence.

In the wake of Shi's conviction, Yahoo made significant changes to its corporate policy to keep similar human rights violations from happening again. MacKinnon is not anti-corporation or anti-regulation, and makes a point of talking about the efforts some governments and Internet companies have made to protect netizens. She also emphasizes the role netizens in the free world can play in promoting a global open Internet. While circumvention software to "climb the wall," anonymizers, and other tools made in the Western world for people living with a less-than-free Internet have their place, we can do the most good for netizens worldwide by making Internet companies at home accountable to us.

American netizens rose to the task earlier this year in their petition against the House's SOPA (Stop Online Piracy Act) and the Senate's PIPA (Protect IP Act), bills which would punish Web platforms allowing copyrighted material to be shared and force Internet service providers and search engines to block access to "rogue websites." On January 18, Wikipedia and other websites coordinated a blackout in protest. The blackouts, petitions, and rallies influenced the postponement of hearings on both bills.

There is plenty of talk about *what* is censored online, but not nearly enough about *how*. To understand why online conversations evolve as they do in China—or Iran, or the US—we need to understand the mechanisms that support those conversations. And to make the Internet free for everyone, we need to start at home.

*Anne Henochowicz is the translation coordinator for China Digital Times. She earned her masters in Chinese literature and folklore from The Ohio State University. She lives in Washington, D.C. You can reach her on Twitter @murasakint.*