Asia Provides Example for Silicon Valley Pressured on Terrorism

Kartikay Mehrotra   Lulu Yilun Chen   Tim Culpan
KartikayM   luluyilun   tculpan
December 9, 2015 — 4:30 PM IST

▶ Government requests in Asia often ``taken as an order''

▶ Companies work with China, India, South Korea authorities

Silicon Valley companies facing a political debate about cooperating with the U.S. government can look to Asia to see how that works in real life.

While Alphabet Inc.'s Google and Twitter Inc. deal with calls to provide encryption back-doors or hand over data to U.S. authorities, some of their Asian counterparts already are pliant. Threats including sectarian violence and political unrest have prompted pressure on Asian online services in a region where freedom of speech rarely has strong constitutional protections like the U.S. with the First Amendment.

Phone and Internet companies operating from China to India to South Korea can see their messaging services censored, content scrubbed or users identified. Whether it's to combat religious tensions or protect the ruling party, those actions can apply to anyone doing business in those countries, including Tencent Holdings Ltd., Facebook Inc. or LinkedIn Corp.

"When a government in this region makes even a gentle request of a company, it's taken as an order," said Rohan Gunaratna, who runs the International Centre for Political Violence and Terrorism Research at Singapore's Nanyang Technological University. "That's a huge difference from the West, where they're so focused on human rights and freedom."

Political Calls

President Barack Obama this week called on U.S. companies to make it harder for terrorists to use technology to escape justice, while Democratic presidential candidate Hillary Clinton urged Silicon Valley to disrupt Islamic State. Those speeches followed the emergence of evidence that social media was used by the militant group in the Paris attacks that killed 130 people.

That's triggering a debate on how far private companies should go in a nation where freedom of speech is paramount.

The situation differs in China, which has long managed the flow of information within its borders, from censoring news and blocking websites to punishing those who overstep the rules. Last year, Ilham Tohti, a blogger from the Muslim minority group known as Uighurs, was convicted of inciting "separatism" and sentenced to life in prison despite views the Committee to Protect Journalists characterized as moderate.

Separatist activity in the Xinjiang region, home to the Uighurs, prompted drastic action, with the central government taking control of instant-messaging services in the city of Hotan last year, Caixin reported, citing a government notice. The country has also severed Internet access, such as in 2009 after people were killed during a knife attack blamed on separatists, according to the official Xinhua News Agency.

Sectarian Battle

"Internet companies play a unique and important role in the war against terrorism," said Li Wei, head of security and anti-terrorism research at the China Institutes of Contemporary International Relations in Beijing. Yet "when Internet companies join the fight in terrorism, it might hurt user privacy protection in some ways."

The oversight is being escalated with plans to dispatch police officers to staff "security offices" within major Internet companies. That includes Tencent, operator of the WeChat and QQ messaging services with more than 1 billion combined users, and search-engine owner Baidu Inc.

Baidu representatives declined to comment when contacted by e-mail. Canny Lo, a spokeswoman for Shenzhen-based Tencent, didn't answer a phone call, a voice mail, e-mails and text messages asking how the company responds to government requests concerning terrorism.

India Violence

In India, a sectarian divide between Hindus, Muslims and other groups has fueled decades of violence. Security agencies work regularly with telecommunications providers and social-media companies to investigate potential threats, according to an Indian intelligence official who wasn't authorized to speak publicly about the issue.

In 2012, India blocked 65 websites and censored what it called "inflammatory and harmful content" content on Facebook and Twitter in its biggest clampdown on social media in at least four years following violence between an indigenous tribe and Muslims. A 2008 law allowed the government to block websites and required companies to designate a point of contact for official requests, yet having the legislation in place is considered only a first step.

"With ISIS warning that they're ready to expand into India, we need to crack down," said Pavan Duggal, founder of CyberLaw India. "It's far more complicated than getting tech firms to cooperate. India needs a holistic national approach for how to deal with online terrorism and online activity leading to terrorism, which is currently non-existent."

Officials in South Korea, a country still technically at war with North Korea, keep a watchful eye over the reclusive neighbor. A cyber-attack last year that was blamed on North Korea targeted South Korean banks and other sensitive institutions.

North Korea

According to democracy advocate Freedom House, service providers in South Korea cooperate extensively with government agencies. Those include popular messaging services such as Kakao Corp.'s Kakao Talk and Naver Corp.'s Line.

"Internet users face censorship rooted in political tensions with North Korea or traditional social values, and numerous laws restrict different aspects of digital activity," said the advocacy group, whose sponsors include Google and the U.S. government. South Korean censors first warn users to delete "harmful" posts before asking service providers to block accounts, it said in a report this year.

Naver fully cooperates with the government based on "legal standards," said Nam Ji Woong, a spokesman for the company. Kakao doesn't hand over user data without proper legal documentation, said Kane Lee, a spokesman for the company.

Local laws don't only affect local operators. U.S. companies operating in a country must abide by those same requirements. LinkedIn, for example, allows censorship on its Chinese service.

Facebook, Google and Apple representatives didn't respond to requests for comment. A U.S.-based Twitter spokesman, Nu Wexler, said the company deals no differently with Asia governments than it does with U.S. authorities.

"If Internet companies work with the U.S. to fight terrorism, they should consider working with all countries across the globe to achieve better results," the China Institutes' Li said.

Before it's here, it's on the Bloomberg Terminal.

• Terrorism • Asia • India • Tech • Internet • China