TECHNOLOGY

India democracy questioned on spyware and data bill

WhatsApp users were allegedly targeted by tool developed by Israeli startup

KEN KOYANAGI, Editor-at-large, Nikkei Asian Review

December 25, 2019 16:19 JST

MUMBAI -- Israeli spyware startup NSO Group proclaims on its website that it "creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe."

Its stated ideal may be so. But its flagship Pegasus is spyware that intercepts communications or location information via mobile phones. Venture capital and private equity funds had invested in the company since its founding in 2010 as if it were a regular startup. But those investors have begun to realize that many of its business dealings border on illegality. This year, the founders' group repurchased a majority stake.

The most serious question about NSO's ethical grounding was raised when it was alleged in late 2018 to have sold Pegasus to the Saudi Arabian regime and helped it spy on a friend of Jamal Khashoggi, the dissident Saudi journalist murdered at the Saudi Consulate in Istanbul that October. The friend sued the company in Israel over that allegation, which NSO claims to be groundless, and he told U.S. media that he believed that the information collected from his phone led to the Saudis' decision to kill the journalist.

In fact, every time Pegasus has been under the spotlight over the past several years, it has been because of allegations that the spyware has been used to monitor anti-government activists, journalists and civil rights activists, rather than for legitimate law enforcement activities. The countries on its "customer" list have been always those with a reputation for human rights violations -- the United Arab Emirates, Mexico and Panama, in addition to Saudi Arabia, for example.

But in October this year, the world's largest democracy, India, became ensnared in the spyware controversy.

American chat platform WhatsApp and parent Facebook took NSO Group to federal court in California, alleging that the Israeli developer sent the spyware to the mobile phones of about 1,400 WhatsApp users. WhatsApp later said about 120 of the targets were residents of India, with at least two dozen of them being journalists, human rights activists and others with political influence. Their phones were hacked around April and May, it said -- the months of the lower house elections.

NSO says it sells only to governments. If so, then who but the government of Prime Minister Narendra Modi could have been spying on the communications of Indian journalists and activists via Pegasus? Ravi Shankar Prasad, the electronics and information technology minister who had come down hard on WhatsApp over preventing false rumors, has become the target of intense questioning by opposition party members and media organizations.

As such suspicions swirled, the Modi cabinet on Dec. 11 submitted to Parliament the Personal Data Protection Bill requiring tech companies to obtain user consent to collect and use their information -- similar to the European Union's General Data Protection Regulation.

The legislation move did not draw much notice initially, because it was submitted the day Parliament passed the controversial Citizenship (Amendment) Bill -- which grants Indian citizenship to immigrants from neighboring countries so long as they are not Muslim -- sparking nationwide street protests claiming that the law discriminates against Muslims and violates the secular principles upheld by the country's constitution.

But the data bill is gradually raising concerns, as one of its provisions says the central government can exempt any of its agencies from its stipulations in the interest of "security of state," "public order," and the "sovereignty and integrity of India." The authorities would thus be enabled to force the likes of Facebook, WhatsApp and Google to supply personal information, including communications collected by their apps. It would amount to a compromise of the principle of secrecy of correspondence, an indispensable pillar of a democratic political system.

This would legalize what has been considered off-limits under India's current laws, even sparing the government from having to surreptitiously use spyware. Such Asian countries as Vietnam, Singapore and Thailand -- which prioritize order and regime stability over freedom of speech and freedom of political activity -- seem to be following in the footsteps of China, which has built the world's first and most powerful nationwide online surveillance network, by stepping up to establish legal and regulatory frameworks that authorize them to demand data from domestic and foreign tech companies alike.

Should the new data bill pass Parliament to become law as is, it could mark a fundamental shift in India's position in the world's human rights and political freedom rankings. And that would surely reinforce the trend of democratic regression in the region.