How surveillance works in India

Pranesh Prakash

2013-07-10

New York Times - India Ink

Abstract

There is a strange mix of great amounts of transparency and very little accountability when it comes to surveillance and intelligence agencies.

When the Indian government announced it would start a Centralized Monitoring System in 2009 to monitor telecommunications in the country, the public seemed unconcerned. When the government announced that the system, also known as C.M.S., commenced in April, the news didn't receive much attention. After a colleague at the Centre for Internet and Society wrote about the program and it was lambasted by Human Rights Watch, more reporters started covering it as a privacy issue. But it was ultimately the revelations by Edward J. Snowden about American surveillance that prompted Indians to ask questions about its own government's surveillance programs.

In India, we have a strange mix of great amounts of transparency and very little accountability when it comes to surveillance and intelligence agencies. Many senior officials are happy to anonymously brief reporters about the state of surveillance, but there is very little that is officially made public, and still less is debated in the national press and in Parliament.

This lack of accountability is seen both in the way the Big-Brother acronyms (C.M.S., Natgrid, T.C.I.S., C.C.T.N.S., etc.) have been rolled out, as well as the murky status of the intelligence agencies. No intelligence agency in India has been created under an act of Parliament with clearly established roles and limitations on powers, and hence there is no public accountability whatsoever.

The absence of accountability has meant that the government has since 2006 been working on the C.M.S., which will integrate with the Telephone Call Interception System that is also being rolled out. The cost: around 8 billion rupees ($132 million) — more than four times the initial estimate of 1.7 billion — and even more important, our privacy and personal liberty. Under their licensing terms, all Internet service providers and telecom providers are required to provide the government direct access to all communications passing through them. However, this currently happens in a decentralized fashion, and the government in most cases has to ask the telecoms for metadata, like call detail records, visited Web sites, IP address assignments, or to carry out the interception and provide the recordings to the government. Apart from this, the government uses

equipment to gain access to vast quantities of raw data traversing the Internet across multiple cities, including the data going through the undersea cables that land in Mumbai.

With the C.M.S., the government will get centralized access to all communications metadata and content traversing through all telecom networks in India. This means that the government can listen to all your calls, track a mobile phone and its user's location, read all your text messages, personal e-mails and chat conversations. It can also see all your Google searches, Web site visits, usernames and passwords if your communications aren't encrypted.

You might ask: Why is this a problem when the government already had the same access, albeit in a decentralized fashion? To answer that question, one has to first examine the law.

There are no laws that allow for *mass* surveillance in India. The two laws covering interception are the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, as amended in 2008, and they restrict lawful interception to time-limited and targeted interception.The targeted interception both these laws allow ordinarily requires case-by-case authorization by either the home secretary or the secretary of the department of information technology.

Interestingly, the colonial government framed better privacy safeguards into communications interception than did the post-independence democratic Indian state. The Telegraph Act mandates that interception of communications can only be done on account of a public emergency or for public safety. If either of those two preconditions is satisfied, then the government may cite any of the following five reasons: "the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, or public order, or for preventing incitement to the commission of an offense." In 2008, the Information Technology Act copied much of the interception provision of the Telegraph Act but removed the preconditions of public emergency or public safety, and expands the power of the government to order interception for "investigation of any offense." The IT Act thus very substantially lowers the bar for wiretapping.

Apart from these two provisions, which apply to interception, there are many laws that cover recorded metadata, all of which have far lower standards. Under the Code of Criminal Procedure, no court order is required unless the entity is seen to be a "postal or telegraph authority" — and generally e-mail providers and social networking sites are not seen as such.

Unauthorized access to communications data is not punishable per se, which is why a private detective who gained access to the cellphone records of Arun Jaitley, a Bharatiya Janata Party leader, has been charged under the weak provision on fraud, rather than invasion of privacy. While there is a provision in the Telegraph Act to punish unlawful interception, it carries a far lesser penalty (up to three years of imprisonment) than for a citizen's failure to assist an agency that wishes to intercept or monitor or decrypt (up to seven years of imprisonment).

To put the ridiculousness of the penalty in Sections 69 and 69B of the IT Act provision in perspective, an Intelligence Bureau officer who spills national secrets may be imprisoned up to three years. And under the Indian Penal

Code, failing to provide a document one is legally bound to provide to a public servant, the punishment can be up to one month's imprisonment. Further, a citizen who refuses to assist an authority in decryption, as one is required to under Section 69, may simply be exercising her constitutional right against self-incrimination. For these reasons and more, these provisions of the IT Act are arguably unconstitutional.

As bad as the IT Act is, legally the government has done far worse. In the licenses that the Department of Telecommunications grants Internet service providers, cellular providers and telecoms, there are provisions that require them to provide direct access to all communications data and content even without a warrant, which is not permitted by the existing laws on interception. The licenses also force cellular providers to have 'bulk encryption' of less than 40 bits. (Since G.S.M. network encryption systems like A5/1, A5/2, and A5/3 have a fixed encryption bit length of 64 bits, providers in India have been known use A5/0, that is, no encryption, thus meaning any person — not just the government — can use off-the-air interception techniques to listen to your calls.)

Cybercafes (but not public phone operators) are required to maintain detailed records of clients' identity proofs, photographs and the Web sites they have visited, for a minimum period of one year. Under the rules designed as India's data protection law (oh, the irony!), sensitive personal data has to be shared with government agencies, if required for "purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offenses."

Along similar lines, in the rules meant to say when an Internet intermediary may be held liable for a user's actions, there is a provision requiring the Internet company to "provide information or any such assistance to government agencies legally authorized for investigative, protective, cybersecurity activity." (Incoherent, vague and grammatically incorrect sentences are a consistent feature of laws drafted by the Ministry of Communications and IT; one of the telecom licenses states: "The licensee should make arrangement for monitoring simultaneous calls by government security agencies," when clearly they meant "for simultaneous monitoring of calls.")

In a landmark 1996 judgment, the Indian Supreme Court held that telephone tapping is a serious invasion of an individual's privacy and that the citizens' right to privacy has to be protected from abuse by the authorities. Given this, undoubtedly governments must have explicit permission from their legislatures to engage in any kind of broadening of electronic surveillance powers. Yet, without introducing any new laws, the government has surreptitiously granted itself powers — powers that Parliament hasn't authorized it to exercise — by sneaking such powers into provisions in contracts and in subordinate legislation.

Pranesh Prakash is Policy Director, The Centre for Internet and Society, Bangalore.

Thursday: Why Indians shouldn't trust the government when it comes to privacy.