Can India trust its government on privacy?

Pranesh Prakash

2013-07-11

New York Times - India Ink

Abstract

The limited efforts to make India's intelligence agencies more accountable have gone nowhere.

> **Note**
>
> This is the second of a two-part series. See the first part here: How surveillance works in India.

In response to criticisms of the Centralized Monitoring System, India's new surveillance program, the government could contend that merely having the capability to engage in mass surveillance won't mean that it will. Officials will argue that they will still abide by the law and will ensure that each instance of interception will be authorized.

In fact, they will argue that the program, known as C.M.S., will better safeguard citizens' privacy: it will cut out the telecommunications companies, which can be sources of privacy leaks; it will ensure that each interception request is tracked and the recorded content duly destroyed within six months as is required under the law; and it will enable quicker interception, which will save more lives. But there are a host of reasons why the citizens of India should be skeptical of those official claims.

Cutting out telecoms will not help protect citizens from electronic snooping since these companies still have the requisite infrastructure to conduct surveillance. As long as the infrastructure exists, telecom employees will misuse it. In a 2010 report, the journalist M.A. Arun noted that "alarmingly, this correspondent also came across several instances of service providers' employees accessing personal communication of subscribers without authorization." Some years back, K.K. Paul, a top Delhi Police officer and now the Governor of Meghalaya, drafted a memo in which he noted mobile operators' complaints that private individuals were misusing police contacts to tap phone calls of "opponents in trade or estranged spouses."

India does not need to have centralized interception facilities to have centralized tracking of interception requests. To prevent unauthorized access to communications content that has been intercepted, at all points of time, the

files should be encrypted using public key infrastructure. Mechanisms also exist to securely allow a chain of custody to be tracked, and to ensure the timely destruction of intercepted material after six months, as required by the law. Such technological means need to be made mandatory to prevent unauthorized access, rather than centralizing all interception capabilities.

At the moment, interception orders are given by the federal Home Secretary of India and by state home secretaries without adequate consideration. Every month at the federal level 7,000 to 9,000 phone taps are authorized or re-authorized. Even if it took just three minutes to evaluate each case, it would take 15 hours each day (without any weekends or holidays) to go through 9,000 requests. The numbers in Indian states could be worse, but one can't be certain as statistics on surveillance across India are not available. It indicates bureaucratic callousness and indifference toward following the procedure laid down in the Telegraph Act.

In a 1975 case, the Supreme Court held that an "economic emergency" may not amount to a "public emergency." Yet we find that of the nine central government agencies empowered to conduct interception in India, according to press reports — Central Board of Direct Taxes, Intelligence Bureau, Central Bureau of Investigation, Narcotics Control Bureau, Directorate of Revenue Intelligence, Enforcement Directorate, Research & Analysis Wing, National Investigation Agency and the Defense Intelligence Agency — three are exclusively dedicated to economic offenses.

Suspicion of tax evasion cannot legally justify a wiretap, which is why the government said it had believed that Nira Radia, a corporate lobbyist, was a spy when it defended putting a wiretap on her phone in 2008 and 2009. A 2011 report by the cabinet secretary pointed out that economic offenses might not be counted as "public emergencies," and that the Central Board of Direct Taxes should not be empowered to intercept communications. Yet the tax department continues to be on the list of agencies empowered to conduct interceptions.

India has arrived at a scary juncture, where the multiple departments of the Indian government don't even trust each other. India's Department of Information Technology recently complained to the National Security Advisor that the National Technical Research Organization had hacked into National Informatics Center infrastructure and extracted sensitive data connected to various ministries. The National Technical Research Organization denied it had hacked into the servers but said hundreds of e-mail accounts of top government officials were compromised in 2012, including those of "the home secretary, the naval attaché to Tehran, several Indian missions abroad, top investigators of the Central Bureau of Investigation and the armed forces," The Mint newspaper reported. Such incidents aggravate the fear that the Indian government might not be willing and able to protect the enormous amounts of information it is about to collect through the C.M.S.

Simply put, government entities have engaged in unofficial and illegal surveillance, and the C.M.S. is not likely to change this. In a 2010 article in Outlook, the journalist Saikat Datta described how various central and state intelligence organizations across India are illegally using off-the-air interception devices. "These systems are frequently deployed in Muslim-dominated areas of

cities like Delhi, Lucknow and Hyderabad," Mr. Datta wrote. "The systems, mounted inside cars, are sent on 'fishing expeditions,' randomly tuning into conversations of citizens in a bid to track down terrorists."

The National Technical Research Organization, which is not even on the list of entities authorized to conduct interception, is one of the largest surveillance organizations in India. The Mint reported last year that the organization's surveillance devices, "contrary to norms, were deployed more often in the national capital than in border areas" and that under new standard operating procedures issued in early 2012, the organization can only intercept signals at the international borders. The organization runs multiple facilities in Mumbai, Bangalore, Delhi, Hyderabad, Lucknow and Kolkata, in which monumental amounts of Internet traffic are captured. In Mumbai, all the traffic passing through the undersea cables there is captured, Mr. Datta found.

In the western state of Gujarat, a recent investigation by Amitabh Pathak, the director general of police, revealed that in a period of less than six months, more than 90,000 requests were made for call detail records, including for the phones of senior police and civil service officers. This high a number could not possibly have been generated from criminal investigations alone. Again, these do not seem to have led to any criminal charges against any of the people whose records were obtained. The information seems to have been collected for purposes other than national security.

India is struggling to keep track of the location of its proliferating interception devices. More than 73,000 devices to intercept mobile phone calls have been imported into India since 2005. In 2011, the federal government asked various state governments, private corporations, the army and intelligence agencies to surrender these to the government, noting that usage of any such equipment for surveillance was illegal. We don't know how many devices were actually turned in.

These kinds of violations of privacy can have very dangerous consequences. According to the former Intelligence Bureau head in the western state of Gujarat, R.B. Sreekumar, the call records of a mobile number used by Haren Pandya, the former Gujarat home minister, were used to confirm that it was he who had provided secret testimony to the Citizens' Tribunal, which was conducting an independent investigation of the 2002 sectarian riots in the state. Mr. Pandya was murdered in 2003.

The limited efforts to make India's intelligence agencies more accountable have gone nowhere. In 2012, the Planning Commission of India formed a group of experts under Justice A.P. Shah, a retired Chief Justice of the Delhi High Court, to look into existing projects of the government and to suggest principles to guide a privacy law in light of international experience. (Centre for Internet and Society, where I work was part of the group). However, the government has yet to introduce a bill to protect citizens' privacy, even though the governmental and private sector violations of Indian citizens' privacy is growing at an alarming rate.

In February, after frequent calls by privacy activists and lawyers for greater accountability and parliamentary oversight of intelligence agencies, the Centre

for Public Interest Litigation filed a case in the Supreme Court. This would, one hopes, lead to reform.

Citizens must also demand that a strong Privacy Act be enacted. In 1991, the leak of a Central Bureau of Investigation report titled "Tapping of Politicians' Phones" prompted the rights groups, People's Union of Civil Liberties to file a writ petition, which eventually led to a Supreme Court of India ruling that recognized the right to privacy of communications for all citizens as part of the fundamental rights of freedom of speech and of life and personal liberty. However, through the 2008 amendments to the Information Technology Act, the IT Rules framed in 2011 and the telecom licenses, the government has greatly weakened the right to privacy as recognized by the Supreme Court. The damage must be undone through a strong privacy law that safeguards the privacy of Indian citizens against both the state and corporations. The law should not only provide legal procedures, but also ensure that the government should not employ technologies that erode legal procedures.

A strong privacy law should provide strong grounds on which to hold the National Security Advisor's mass surveillance of Indians (over 12.1 billion pieces of intelligence in one month) as unlawful. The law should ensure that Parliament, and Indian citizens, are regularly provided information on the scale of surveillance across India, and the convictions resulting from that surveillance. Individuals whose communications metadata or content is monitored or intercepted should be told about it after the passage of a reasonable amount of time. After all, the data should only be gathered if it is to charge a person of committing a crime. If such charges are not being brought, the person should be told of the incursion into his or her privacy.

The privacy law should ensure that all surveillance follows the following principles: legitimacy (is the surveillance for a legitimate, democratic purpose?), necessity (is this necessary to further that purpose? does a less invasive means exist?), proportionality and harm minimization (is this the minimum level of intrusion into privacy?), specificity (is this surveillance order limited to a specific case?) transparency (is this intrusion into privacy recorded and also eventually revealed to the data subject?), purpose limitation (is the data collected only used for the stated purpose?), and independent oversight (is the surveillance reported to a legislative committee or a privacy commissioner, and are statistics kept on surveillance conducted and criminal prosecution filings?). Constitutional courts such as the Supreme Court of India or the High Courts in the Indian states should make such determinations. Citizens should have a right to civil and criminal remedies for violations of surveillance laws.

Indian citizens should also take greater care of their own privacy and safeguard the security of their communications. The solution is to minimize usage of mobile phones and to use anonymizing technologies and end-to-end encryption while communicating on the Internet. Free and open-source software like OpenPGP can make e-mails secure. Technologies like off-the-record messaging used in apps like ChatSecure and Pidgin chat conversations, TextSecure for text messages, HTTPS Everywhere and Virtual Private Networks can prevent Internet service providers from being able to snoop, and make Internet communications anonymous.

Indian government, and especially our intelligence agencies, violate Indian citizens' privacy without legal authority on a routine basis. It is time India stops itself from sleepwalking into a surveillance state.

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