Sunday Interview: "By weakening our security, govt is putting us at risk of espionage"

Pranesh Prakash

2015-09-27

Deccan Chronicle

Abstract

The government intended to gain greater access to everyday transactions

---

After the BlackBerry encryption and IT Act fiascos of recent years, the government last week sent yet another cyber policy howler, the Draft National Encryption Policy, only to withdraw it in the face of severe protests. S. Raghotham and Mayukh Mukherjee spoke with Pranesh Prakash, policy director, Centre for Internet & Society, on the government's continued misadventures with data privacy and encryption.

First we had Section 66A in the Information Technology Act. Now we have these attempts at breaking encryption and invading privacy. Your comment.

The Draft National Encryption Policy (DNEP) was not only an invasion of privacy and a restriction on anonymous speech, but was, most importantly, a direct assault on national security. It was quite clearly drafted by people who did not understand encryption, who think that encryption is something that only a handful of people do, without realising that encryption is baked into most of our technologies.

It is clear that the government's cyber-law division needs people who are better versed in both the law (including constitutional rights) as well as technical aspects of IT. It's not just Section 66A, but a host of other provisions in the IT Act which display a similar cluelessness. For instance, gaining unauthorised access to a protected system for purposes of defamation is, as per Indian law, sufficient to commit the offence of "cyber terrorism".

How does this compare with the previous government's attempts to gain access to BlackBerry communications?

L'affaire BlackBerry concluded with the government realising that while they could get BlackBerry to locate a network operations centre in India, they still couldn't decrypt everything since BlackBerry Enterprise Service allowed enterprises to control the encryption. However, the government seems to have drawn

the wrong lesson from that, and wants to prevent end-users from using encryption the way they have already managed with telecom companies and Internet service providers, who are not allowed to deploy bulk encryption which saves their customers' data from being intercepted by attackers.

The government seems to be saying, if the US National Security Agency (NSA) doesn't get you, we will. How are we to respond to this?

If you're using Gmail, Yahoo Mail, Hotmail, etc., you already have opportunistic traffic-level encryption for email. Ironically, no @deity.gov.in or @nic.in address has even this basic level of encryption. This is the shocking state of affairs even many years after National Informatics Centre (NIC) publicly acknowledged that multiple email accounts that they host were hacked into.

National security is a collective form of security — we can't increase national security by making individuals less secure. We can't, for instance, improve national security by telling people not to use locks on their houses. That will only decrease security, not increase it. And we are in a situation where our government conducts all their email communications using the online equivalent of postcards, rather than using sealed envelopes. The Central government urgently needs to appoint a group of security experts who work with NIC to shore up our defensive security.

A slide on an NSA programme called BOUNDLESSINFORMANT showed that in the month of February 2013, the NSA has collected 12.5 billion data records relating to phone calls from India, far more than what they had collected from China. The fact that our government mandates weak telecom security (by restricting bulk encryption) might account for this. By weakening our security, the government is putting us at greater risk of espionage and at the hands of hackers.

What are some of the ramifications for businesses and individuals if the government were to have keys to all encrypted information as it seeks?

The government, in the DNEP, did not even seek key escrow (which is what the debate was about in the 1990s in the US' "crypto war"). Here the government more or less sought to tell companies and individuals that they have to keep plain text, making storage-level encryption pointless. This means that all your company's information — emails, passwords and financial records — would be vulnerable to compromise by hackers. It is like telling a company that it is allowed to own a government-approved safe for storing important documents, but it has to keep a copy of all the important documents outside the safe.

Is the encryption policy fiasco some junior bureaucrat's ignorance of what he was proposing or is it part of the government's continued efforts to somehow gain control over information flows?

The government intended to gain greater access to everyday transactions. This would violate citizens' privacy, which the government has been arguing is not a fundamental right. They went about it in a manner that is absurd in its consequences. The policy would have required you to record every mobile phone

call and Skype call, to keep a plain text version of communications, which would harm national security.

While I don't believe the government would intentionally weaken national security, as they would have had this draft policy been carried forward, one cannot say that the government wouldn't do so wantonly, much in the same way that they haven't even employed basic security in their email systems.

Do you perceive a higher level of desire in the current government to control information flows?

The Indian government's pursuance of harmful technology policies is nothing new. However, I hope that as a tech-savvy person heading an ostensibly tech-savvy government, Prime Minister Narendra Modi steps in and halts these deleterious policies. One disappointment of the last year has been the lack of progress on the Privacy Act, which seems to have been shelved for the time being. I believe the government's motivations are genuine and grounded in the public interest.

However, as in any constitutional democracy, the citizenry ought to be engaged in both defining the public interest as well as in debating how we best protect and uphold it within the norms laid down in our Constitution, which includes guarantees of fundamental rights which are inviolable except in limited circumstances.

For most of these policy problems, the best way forward is to ensure that the government follow a system of issuing green papers — essentially non-papers meant to stimulate public discussion — before it issues white papers which contain statements of policy intent, based on which it finally formulates policies or laws. Currently, interaction between policymakers and civil society is far too infrequent. The government needs to inject far more subject-matter expertise into policymaking.