

[Databases selected:](#) Multiple databases...

Your phone is a double agent; Your phone connection can be monitored without the operator's consent.

Anonymous. India Today. New Delhi: Dec 20, 2010.

Abstract (Summary)

Your cellphone is actually a double-edged weapon, which could be silently relaying every word you speak to the authorities. Neither you nor the service provider will have an inkling of your handset being compromised. Though illegal, intelligence agencies have used this method of 'active intervention' to tap into phones. It is done by planting a bug electronically in the handset. It can be activated by what is called 'pinging' or sending a fake call to your number.

Full Text (331 words)

(Copyright (c) Living Media India Limited. Not to be reprinted or reused in any way without prior permission of the publisher.)

Your cellphone is actually a double-edged weapon, which could be silently relaying every word you speak to the authorities. Neither you nor the service provider will have an inkling of your handset being compromised. Though illegal, intelligence agencies have used this method of 'active intervention' to tap into phones. It is done by planting a bug electronically in the handset. It can be activated by what is called 'pinging' or sending a fake call to your number. You will not know it, but the unique IMEI number of your phone will be available with the agency, decrypting all communication and accessing a steady stream of sms, call logs and data stored in the phone. Existing technology already allows the constant tracking of a mobile phone through its IMEI number. Now, for the next phase, a discretely planted software called 'roving bug' turns a mobile phone into a bugging device. It can turn on the handset's microphone and stealthily transmit all conversations in its vicinity. This transmission continues even when the phone is switched off. Experts say the only way to stop such a transmission from an infected phone is to pull the battery out.

There is virtually no handset that cannot be tapped. However, intelligence agencies have so far hit a dead end with BlackBerry messenger and Business Enterprise Service (BES). The IMEI number only pinpoints the location of the phone but cannot monitor BES and BlackBerry messenger. The cooperation of the phone's manufacturer Research in Motion (RIM) is required to plant a bug that modifies the operating system of the phone, in either the handset or the BES server.

BlackBerry's most famous user, US President Barack Obama uses a special BlackBerry 8830 with enhanced encryptions. Sanitised to an extent that he could receive messages only from a select group of 10 persons. Closer home, Prime Minister Manmohan Singh and select officials in the pmo use custom-built encrypted mobile phone handsets designed by the DRDO and built by Bharat Electronics Ltd.

Indexing (document details)

Companies:	BlackBerry
Author(s):	Anonymous
Document types:	News
Section:	Cover Story
Publication title:	India Today. New Delhi: Dec 20, 2010.
Source type:	Periodical
ISSN:	02548399
ProQuest document ID:	2217009931
Text Word Count	331

Document URL: <http://proquest.umi.com/pqdweb?did=2217009931&sid=1&Fmt=3&clientId=11561&RQT=309&VName=PQD>

Copyright © 2011 ProQuest LLC. All rights reserved.

