

- [About VpnHero.com](#)
- [Privacy](#)
- [Contact](#)
- [Disclosure](#)



VPNHERO.com

Best VPN Services of 2015 –

VPN Reviews | [VpnHero.com](#) VPN Articles and Reviews



- [Home](#)
- [VPN Reviews](#)
- [VPN Coupon Codes](#)
- [News](#)
- [Articles](#)
- [Tutorials](#)

Categorized | [News](#)

Indian Government to Monitor Facebook and Twitter

Posted on 12 August 2011. Tags: [Facebook](#), [india vpn](#), [indian governement](#), [internet monitoring](#), [twitter](#)

G+1 0



India's Centre for Internet and Society (CIS) now wishes to monitor conversations and exchanges on social networking sites such as Facebook and Twitter. India's Minister of State for Communications and Information Technology, Milind Deora, acknowledged as much, when questioned on it by the Rajya Sabha. The government gaining access to "encrypted data" was spoken about in particular.

The current Indian Telegraph Act, namely the Indian Information Technology (IT) Act 2008 allows the

government to intercept, monitor, and even block both online conversations, as well as entire websites. The list of eleven such websites, which have been blocked by the government, was recently released by the CIS. As the Executive Director of CIS, Sunil Abraham said, “For the first time in India, we have a list of websites that are blocked by order of the Indian government.”

So now, due to their popularity in India, as well as the threat of cybercriminals and terrorists exerting their influence online, the government will also begin closely monitoring social networking sites like Facebook, Twitter, Orkut, and Google+. These are the most popular social networking sites in India at the moment, with millions of people visiting them regularly. These sites have been used successfully to launch countrywide campaigns, such as the one launched by Anna Hazare to unite the public against corruption in India. In the past, social networking sites have also been used to help people during natural disasters like floods and earthquakes.

“The Indian government can, and should, monitor conversations and websites if it believes the content can harm the security, defense, sovereignty and integrity of the country,” said Pavan Duggal, a Supreme Court lawyer and a cyber law expert. Abraham of CIS agrees with this, but neither are sure how to go about implementing this type of monitoring by the government. Duggal went on to add that, “The intention is good but the path is not clear.”

Facebook, Twitter and Google all house their servers outside of India, which raises jurisdiction issues. In Twitter’s guidelines for law enforcement it is, for example, clearly stated that “Non-public information about Twitter users is not released, unless we have received a subpoena, court order, or other valid legal process documents,” with Facebook having a similar policy. Google also has the same policy, though the company has, in the past, worked with the government of India, when the country’s national security was threatened.

However, according to Duggal, sections 1 and 75 of the Indian IT Act, state that any company which operates in India, can be held accountable under Indian law if their practices have an impact computer systems and networks in India, no matter where their headquarters are. However, he went on to say, “But the problem is what would the government monitor on social networking sites—usage of keywords, all users, just the suspects or leave it totally to the service provider?”

The other issue is that under Section 70 (B) of the same Act, ISPs, telecom companies and other service providers must all report cyber security breaches to the government of India, and they face imprisonment should they fail to do so. In addition to this, it is also mandatory for all cybercafés in India to retain the proof of identity of their customers for one year. Though, the government is planning to also introduce a Right to Privacy Bill, which is aimed at protecting their citizens. This bill is said to allow for penalization of “unauthorized interception”, even if the government is the transgressor. This would, according to Duggal pose “Many legal challenges if the government does not go about its task of monitoring users in a transparent manner.”

Abraham of CIS pointed out that, “It’s okay if the government takes this (monitoring of sites) on a case-to-case basis—that is, addressing perceived threats to the country’s security or monitoring conversations that have a pattern leading to a possible attack. But what if it leads to blanket surveillance?” He is of the opinion that this type of surveillance would be very costly. Also, cybercriminals and terrorists use codes when speaking to each other, meaning that code breakers would have to be employed to decipher them. “Moreover, if users of social networking sites feel they are being watched, they would resort to using pseudonyms, encryption or even anonymiser tools to camouflage their identities. There will be a sense of distrust (of the government),” Abraham went on to say.

India has been known to put pressure on companies for access to communications data in the past. They

are not alone in this, as Iran, Egypt, China, and others, have also been known to censor YouTube, Gmail, Research in Motion (RIM), Wikileaks, Twitter, and Facebook, alongside India.

Link

- [India VPN Services](#)

 Tweet
  Like
  Share
 Sign Up to see what your friends like.

 G+1
  0

Related Posts Top 10 VPN Services

- [Internet Censorship in India Still Going Strong](#)
- [Proposed Internet Censorship in India](#)
- [Anti-Internet Censorship Protests Gaining Momentum in India](#)
- [“Free Internet” Non-Existent in India?](#)
- [Google Hacks Apple’s Safari Browser to Install Tracking Cookies](#)
- [An Unlikely Twitter User: A Supporter of Chinese Internet Censorship](#)
- [AT&T Routes USA Facebook User Data via China & Korea](#)
- [Could China Buy Facebook \(And Why\)?](#)

- 1. **ExpressVPN** - 21 Locations - From \$9.99 / mo.
- 2. **StrongVPN** - 19 Locations - From \$4.58 / mo.
- 3. **PureVPN** - 17 Locations - From \$6.00 / mo.
- 4. **VyprVPN** - 6 Locations - From \$14.99 / mo.

Zemanta

- 5. **IAPS Security** - 145 Locations - From \$24.95 / mo.
- 6. **OverPlay** - 28 Locations - From \$9.95 / mo.
- 7. **ibVPN** - 7 Locations - From \$3.08 / mo.
- 8. **HideMyAss** - 32 Locations - From \$6.57 / mo.
- 9. **HideIPVPN** - 3 Locations - From \$5.99 / mo.
- 10. **iVPN** - 2 Locations - From \$10.42 / mo.

VPN Services by Destination Location

Destination

- **Popular**
- Latest
- Subscribe

-  [Apple Hit by Facebook Hackers](#) February 21, 2013
-  [Introduction to VPN Softwares & Protocols](#) January 31, 2011
-  [What is VPN Tunneling?](#) February 1, 2011
-  [What is a VPN?](#) February 2, 2011
-  [What is the Difference Between a Proxy and a VPN?](#) February 3, 2011

Best VPN Service Promos

- StrongVPN - Get a Second VPN Account For Only \$2.00
- Overplay Coupon - Get 15% Off
- ibVPN Coupon Code - Get 50% Discount
- HideMyAss Coupon - Up to 60% Off!
- Strong VPN Coupon - Euro-America Special OpenVPN or PPTP Only \$85/year
- StrongVPN Coupon - 4 City Special PPTP Only \$55/year
- StrongVPN Promo - 4 City Special Open or PPTP Only \$85/year



© 2016 VpnHero.com