

JASON OVERDORF

ARTICLES BY A BERLIN-BASED JOURNALIST

SUNDAY, JANUARY 02, 2011

Industrial espionage booming in corporate India

Insiders say government phone taps are just the tip of the iceberg.

By Jason Overdorf
(GlobalPost - January 2, 2011)

NEW DELHI, India — For the past month, Indian business leaders have watched in horror as a series of tapped telephone conversations between a powerful lobbyist and top industrialists have surfaced in the press.

But local security experts say the revelations associated with the alleged 2G telecom scam are just the tip of the iceberg when it comes to vulnerable company secrets. In India's fast-growing economy, they say, no industry is booming bigger than corporate espionage.

"If you look at all the companies doing business in the electronic sector in India, the chances are that four out of 10 would invariably have faced or are facing such issues," said Pavan Duggal, a supreme court lawyer who specializes in cyber law. "The reality is that these thefts of intellectual property rights and confidential data are hitting the corporate world in a big way."

Cut-throat competition provides ample motive, as companies battle to carve out brand positions, retain top talent and develop new products. A lax legal environment allows spies to operate with relative impunity. And a boom in white collar jobs means that employees shift jobs every few months — making it all too easy for companies to plant a mole in competing operations, and all too tempting for job-jumpers to walk away with sensitive information or protected intellectual property.

"The perpetrators of unauthorized access of corporate data do it with impunity, knowing full well that the law is deficient and that it will take a long time for them to be prosecuted," said Duggal.

GREATEST HITS

- [Dead men working - GlobalPost](#)
- [Physical Culture - The Atlantic](#)
- [Saving the Raja's Horse - Smithsonian](#)
- [Delhi's war on the poor - The Asian Wall Street Journal](#)
- [Women on top - Monocle](#)
- [White Man's Burden - Far Eastern Economic Review](#)
- [Sirrh, Master, Sahib, Boy! - The Asian Wall Street Journal](#)
- [Rebel Brides and Ex-wives - Newsweek International](#)

VIDEOS

- [Himalayan tsunami - GlobalPost](#)
- [Gender equality in India's workplace - GlobalPost](#)
- [Cat fight - GlobalPost](#)
- [India's looming food crisis - GlobalPost](#)
- [India: armed and dangerous - GlobalPost](#)

ABOUT ME



 JASON OVERDORF

 [Follow](#)

[VIEW MY COMPLETE PROFILE](#)

BLOG ARCHIVE

According to a recent survey conducted by the consultancy firm KPMG, 14 percent of Indian companies have been victims of corporate spying, while another 39 percent fell prey to intellectual property theft and computer-related fraud — and business-sensitive information and user IDs/passwords were the principal targets.

The potential losses from this kind of spying are difficult to calculate — since nobody knows what effect a stolen ad campaign might have had, or how a stolen design might have dominated the market. But there's no doubt that big money is at stake. Early this year, for instance, India's Thermax agreed to pay Pennsylvania-based Puro-lite International \$38 million to settle a lawsuit over the alleged theft of proprietary water purification technology.

"You may not use [your competitor's] research work," said Kunwar Vikram Singh, president of the Indian Council of Corporate Investigators. "But suppose you have already developed your own brilliant idea. Even to launch that brilliant idea in the shape of a product you must know the market."

The spies aren't always after new technology. The targeted information ranges from client lists to proprietary software to advertising strategies, says Singh.

Not long ago, for instance, a company was readying a new ad blitz when, on the day before the launch, executives saw their planned slogan all over the city on their morning commute — on billboards advertising one of their competitors.

In another case, one of the country's foremost motorcycle and scooter manufacturers lost the design and specifications for an upcoming model to a competitor through a spy planted with the contractor that was running the company cafeteria.

"They planted a guy ... who knew a little about IT and could become friendly with people, and then when the office was closed he would access employees' computers and get the information out," said Ravi Kapur of ACE Detectives, the private investigator hired to plug the leak.

Part of the problem is that Indian laws governing these areas are weak and ambiguous. India has no specific data protection law, so the theft of sensitive information like marketing strategies or employee salaries — which is not governed by intellectual property laws — throws up a host of legal questions.

- ▶ [2016](#) (2)
- ▶ [2015](#) (11)
- ▶ [2014](#) (78)
- ▶ [2013](#) (33)
- ▶ [2012](#) (29)
- ▼ [2011](#) (60)
 - ▶ [December](#) (6)
 - ▶ [November](#) (6)
 - ▶ [October](#) (5)
 - ▶ [September](#) (5)
 - ▶ [August](#) (4)
 - ▶ [July](#) (5)
 - ▶ [June](#) (7)
 - ▶ [May](#) (3)
 - ▶ [April](#) (6)
 - ▶ [March](#) (3)
 - ▶ [February](#) (4)
 - ▼ [January](#) (6)

[India's "black money" trail](#)

[India: Can tourism trickle down?](#)

[India's red-hot art scene](#)

[India's military shopping spree](#)

[Food crisis threatens India](#)

[Industrial espionage booming in corporate India](#)

- ▶ [2010](#) (53)
- ▶ [2009](#) (44)
- ▶ [2008](#) (31)
- ▶ [2007](#) (26)
- ▶ [2006](#) (14)
- ▶ [2005](#) (27)
- ▶ [2004](#) (14)
- ▶ [2003](#) (18)
- ▶ [2002](#) (11)
- ▶ [2000](#) (1)

And while the unauthorized downloading or copying of computer files is illegal, the civil and criminal penalties are minor compared with the sums at stake for corporations. A criminal booked for data theft under the Information Technology Act, for instance, faces a maximum three-year term in prison and a maximum fine of around \$10,000, and the most a victim can seek in civil damage is about \$1 million — which the Thermax-Purolite settlement reveals as a pittance.

"It's extremely lax," said Kapur. "People don't generally get caught. Then, even if this guy gets caught, they're not after this guy [who took the information] — they're after the competitors. Now, to ensure that the whole chain gets into the loop is not the easiest of tasks."

Private investigators have been the biggest beneficiaries, as the budding industry profits from both sides of the information war. While none of the detective agencies interviewed would admit to conducting actual corporate espionage, firms that perform similar work — such as planting spies for clients within labor unions — say that they get requests to steal competitive information on a daily basis.

Moreover, there's almost as much money to be made in protecting firms from spies as there is from spying on them, not only through investigating leaks, but also in risk analysis, security systems design and — since it's the enemy inside that's most feared — employee background checks.

And that means going to work for an outsourcing company is starting to seem like applying to the Pentagon.

"Before, people were reluctant to snoop around," said Singh. "Now, they go deep."

Copyright 2010 GlobalPost – International News

Source URL -

<http://www.globalpost.com/dispatch/india/101223/industrial-espionage-corporate-india>

POSTED BY [JASON OVERDORF](#) AT 11:24 PM

[Newer Post](#)

[Home](#)

[Older Post](#)