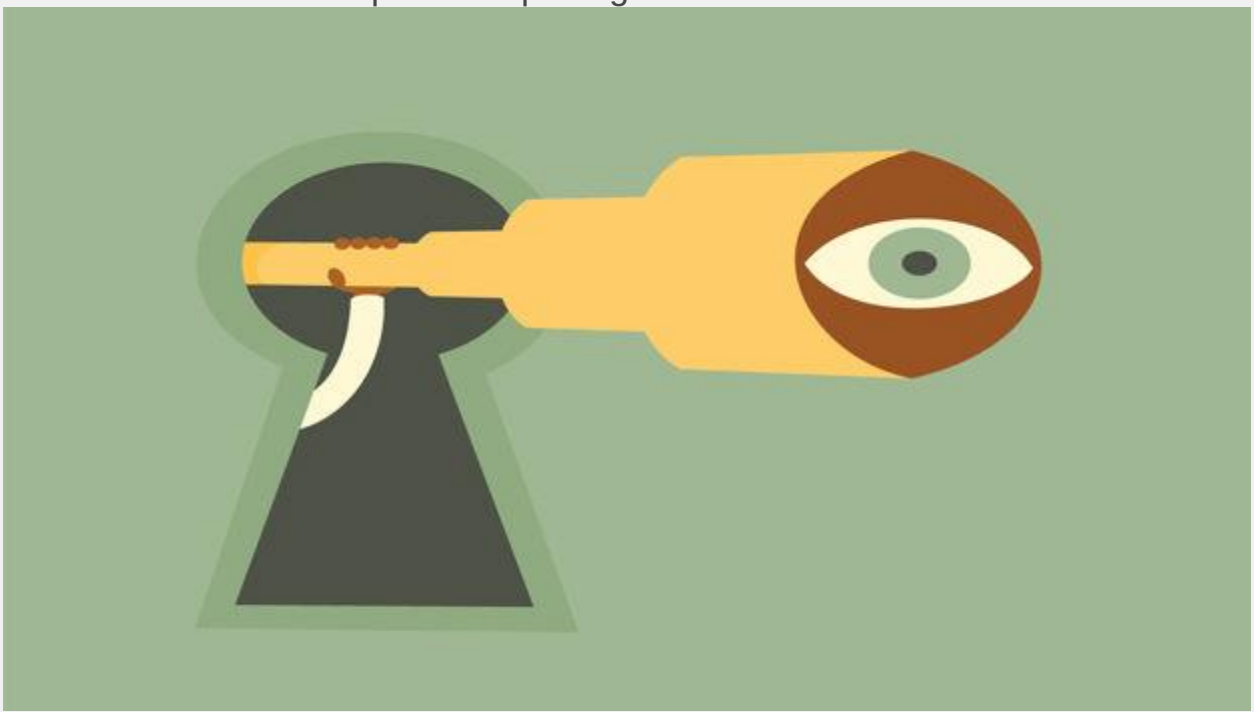
Corporate Espionage or Competitive Intelligence?

Firms must focus on innovation rather than information arbitrage, while there is a need for robust corporate espionage laws



Anu Kurian, Pallavi Sharma

While reconnaissance in India is heavily dependent on government documents, in the US and Europe companies spy on each other to gain an edge in business

Espionage in India dates as far back as to the age of Kautilya, an Indian political philosopher who believed that indulgence in unethical practices in statecraft is justifiable

From the 1700s to the present day, corporate espionage has been a problem for businesses worldwide. Stealing trade secrets is as old as trade itself; it gave rivals to go one up on their game hoodwinking their competition, the regulators and the public in general. In order to protect business interests, laws were brought into place, competition watchdogs set up and stiff penalties imposed. But, history has shown that these have not had the desired impact on the business world. Companies have spied on each other (some even hired a detective agency), employees have stolen confidential documents and sold it to the direct competitor and in some cases they stole proprietary information. While there is an urgent need to make the laws surrounding corporate espionage more robust, companies themselves need to focus on innovation rather than information arbitrage. But, more on that later. The latest episode of corporate espionage to hit the country is PetroLeaks.

It all started when National Security Advisor Ajit Doval raised an alarm that many confidential matters pertaining to government documents were being reported by the media. A four-month long probe followed this and it ultimately led to the corporate espionage scandal involving the Ministry of Petroleum and Natural Gas. Departments of Defence, Power and Coal also faced corporate infiltration in some form. After a line of raids and official interceptions of many phone calls, the Delhi police made its first five arrests (two officials from the ministry of Petroleum and Natural Gas, an employee of Reliance Industries and two middlemen) on February 19 for stealing and leaking classified government data. Companies allegedly associated with arbitrage of government documents in this scandal include industry giants Dhirubhai Ambani Group (R –ADAG), Reliance Industries (RIL), Essar, Cairn India, Jubliant Energy and ONGC.

After the Delhi Police's probe, it was revealed that many confidential government documents were arbitraged, including a piece on the finance minister's budget speech, documents pertaining to coal block allocations, CAG report on hydrocarbon production, Cabinet note on open licencing policy for oil companies and government files pertaining to decisions on several national and international projects.

The total number of arrests made by the Delhi police in the case went up to as many as 14. With many raids being conducted by the Crime Branch, it was also reported that many companies under the police radar extensively went on to hire services of companies who delete data beyond retrieval.

Corporate or industrial espionage is not a new phenomenon in India. Documents are regularly leaked from ministries, government authorities, banks and so on. Cabinet notes, ministries opinions, action planned by RBI, SEBI and even international regulators, banks, income-tax authorities, stock exchanges and even public sector units make their way to the hands of companies through their lobbyists. They use the information thus gathered for a variety of reasons and like making a quick buck at the stock markets or use it to further their business. Here is a snapshot of the some of the major corporate espionage cases:

Radia tape leaks (2008-09): The income tax department had taped conversations between Niira Radia, an influential PR person, and senior journalists, politicians and corporates, the transcripts of which were published by Open Magazine in November 2010. The tapes revealed that Radia had used her media influence to ensure the appointment of A. Raja as the Telecom Minister. She was also heard brokering deals in 2G spectrum that involved allocation of 2G licences to telecommunication operators. However, this eventually led to the 2G spectrum scam, which had resulted in a loss of US $4.9 billion for the Union government.

Industry giants involved in the case were Reliance Telecom, Tata Telecommunications, Swan Telecom and Unitech Wireless. Other famous names associated with the scandal include reputed journalists Barkha Dutt and Vir Sanghvi, politicians A. Raja and Kanimozhi, businessmen Ratan Tata, Mukesh Ambani and Kalanithi Maran.

Tata Telecommunications (2007): Tata Telecommunications filed a case against its Managing Director's secretary who was found sharing the board meeting agendas with Tata Telecommunications' competitor. Barring filing a chargesheet against the employee, Mumbai police failed to crack the case.

The gas war and crony capitalism: After discovery of petroleum and natural gas in the Krishna-Godavari basin, the Government of India opened up hydrocarbon exploration and production in the country to private and foreign players in 1991. This was followed by creation of New Exploration and Licensing Policy (NELP) in 1999 through which Reliance gained access to explore the Krishna-Godavari Dhirubhai-6 site. A production-sharing contract was signed between the government of India and Reliance Industries for exploration and production of oil and gas.

However, after the death of Dhirubhai Ambani, the two Ambani sons split the Reliance group. Mukesh Ambani took over the gas business of the company following which a legal dispute between the pricing of gas between their respective companies arose. Following the rivalry between the Ambani brothers, the Comptroller and Auditor General of India released a report that highlighted how the government had issued favourable contracts to RIL. It is also believed that the portfolio of Petroleum Ministry was frequently distributed among different politicians to favour RIL. Many sensitive information and confidential documents from the RBI and the Securities and Exchange Board of India were leaked during the years that saw the "Gas War" between the Ambani brothers. The whole scandal brought into light how crony capitalism was deeply rooted in the Indian polity.

Corporate Espionages carried out abroad, on the other hand, are of very different character. From companies who wanted to know the trade secrets of their competitors, to disgruntled employees sending confidential documents, to even hiring an investigative agency to prove a point, there are several such cases. See: 10 most notorious corporate espionage cases in the world.

The Tata Telecommunications case is probably the only case in Indian history where an employee was held responsible for spying. While reconnaissance in India is heavily dependent on government documents, in the US and Europe companies spy on each other to gain an edge in business. The main reason behind this difference is the fact that business success in India is driven by information leverage rather than innovation. Dr. Umashanker Venkatesh, Professor, Marketing, Great Lakes Institute of Management argues, "India Inc. runs greatly on secrecy of information. Inaccessibility to crucial information results in prevalence of arbitrage over innovation." The laws in India are highly stringent and government information is kept secret; there is little transparency when it comes to passing of rules and regulations that are capable of impacting decisions of business firms. As a result many resort to crony capitalism or espionage by leveraging political connections.

Almost all of the big espionage cases in India have involved leakage of government documents and files. A business ecosystem based on the ability to compete will bring a different shape to espionage in the country. This will be possible only in two-ways—both the government and corporates evolve when it comes to dealing with espionage. The government, on one hand, needs to bring about transparency, while companies need to focus on innovation rather than information arbitrage. Further, the government needs to frame more stringent and robust laws that will help prevent

corporate espionage. As of now, the only Act that comes close to dealing with such cases is the Information Technology (Amendment) Act, 2008, which includes provisions relating to data protection, privacy, cyber terrorism etc.

Espionage in India dates as far back as to the age of Kautilya, an Indian political philosopher who believed that indulgence in unethical practices in statecraft is justifiable. According to Prof. Venkatesh, the same logic applies to corporates. A business ecosystem without reconnaissance is nothing but a utopia. Unscrupulous practices to gain advantage over a competitor are a part of human behaviour; they take place not only in business, but also in statecraft, education system, or even in the minuscule unit within families.

With the world becoming more connected, companies need to ramp up their data security manifold. From 2006 onwards, over 70 companies, governments and NGOs were hacked by spies and stole information. The attack was traced to China. In 2009, hackers stole proprietary information from six US and European energy companies, including Exxon Mobil, Royal Dutch Shell, and BP. Another more recent one in 2010 saw hackers launching a sophisticated cyberattack on gmail and stole the company's intellectual property.

Many companies are taking various steps to prevent becoming victims of espionage. They have become very strict about security within office premises, board meetings are held in secret away from office and access to top offices are also limited to a few personnel only. The convenience of wireless networks has also brought with it the headaches of security. So more companies are now conducting wireless assessments to ensure that information is not leaked through a wireless network hole. Penetration tests to check the validity of the security, having a security culture in the organization and conducting regular security audits will go a long way in helping companies protect data. So, while companies will continue to engage in espionages, the character of such espionages needs to evolve and take the form of competitive intelligence. Spying on the competitor may help the company gain invaluable secrets, but they will produce only short-term results, not to mention the loss of reputation and employer brand image when they are caught red-handed. Through innovation, companies can focus on long-term profits and plans that would take them into the next league.