VINTELL

MAY 2017, ISSUE 32

A PERSPECTIVE ON DEFENDING AGAINST UNWELCOME PROBING

CONTENTS

BACKGROUND

The headlines speak volumes: Donald Trump Adviser Roger Stone Admits Contact With Suspected Russian Hacker; The Rise Of Industrial Espionage In SA; VW Agrees To Pay G.M. $100 Million In Espionage Suit; Alleged Global Espionage In SA's Tobacco Industry Exposed; Israeli Agents Raid Cape Strawberry Fields; Trade Secret Theft, Industrial Espionage, And The China Threat; Corporate Theft Strikes Fortune 500 Oil Company In Houston; U.S. Charges Six Chinese Citizens With Economic Espionage ...

For as long as there has been commerce, there has been espionage. The methods for spying on competitors have changed over time, but the desire to uncover a rival's secrets has not. Stories about Espionage somehow always peaks an interest whether it is government spying on and outdo one another or stories about companies spying on one another. They make great conversation topics and sometimes we walk away wondering whether our competitors are spying on us. A safe assumption if you are a strong player in a competitive industry is that they are often in unexpected ways and guises. Also in South Africa snooping and spying among competitors is rife. This edition of VinIntell provides a brief overview of present day industrial espionage and competitor monitoring and concludes by offering a few hints at how to neutralise unwelcome probing and defend your own competitive intelligence.

INTRODUCTION

Business headlines warn about international corporate espionage efforts focused against companies and companies' efforts to protect themselves against these illegal activities. However, we must assume that not only companies are targeted: Individuals working for companies are equally targeted. Those efforts, if successful, can also be competitively damaging. In order to protect against unwelcome and potentially harmful probing, you have to understand how competitive intelligence works and how you can, with a few simple steps, create a program to protect competitively sensitive information or data from others. Let us have a brief look at what industrial espionage and its ethical, legal and tamer cousin Competitive Intelligence (CI) are about:

Industrial espionage may not be the oldest profession, but is certainly not a new phenomenon. In biblical times Moses sent spies to Canaan to gain intelligence on agricultural production. The Celts stole methods for improving chariot wheels from the Romans, whilst the Roman emperor Justian used Persian monks to steal the secrets of silk from China. During the industrial revolution in 19th century England the export of technology and also the immigration of people with knowledge of the technology was forbidden. However, Samuel Slater memorised the blue prints of cotton spinning machinery in 1789, boarded a ship for the United States and established the textile industry in New England when he arrived there. The British, in turn, stole and illegally exported rubber plants

from Brazil and cultivated it in the British colony of Malaysia. For the purpose of this edition of VinIntell we shall consider industrial espionage to be espionage activity that is beneficial for commercial and economic purposes. Industrial espionage can be aimed at commercial enterprises such as companies, but also at other sources of technological and economic information such as governmental laboratories, government departments and officials. Industrial espionage is used and perpetrated by private parties as well as by governments, in the latter case usually via their various intelligence agencies. Sometimes such government agencies spy for the benefit of national industries and in this regard the Russians, French and Israelis are masters.

Industrial espionage has been defined as "... the unethical/unlawful acquisition of financial/economic/industrial information regarding a target country, institution or company through intelligence services, private companies or foreign multinational companies for the benefit of own industry/economy. Industrial espionage also includes aspects such as industrial disinformation and industrial sabotage. It is important to note that a foreign government is not necessarily responsible to sponsor or coordinate industrial espionage activities." Industrial espionage, on the other hand, is very often perpetrated by one company against another. As the global economic battle heats up, state-sponsored industrial espionage, typically via the various national intelligence services, is also becoming much more accentuated.

Looking at CI, Ben Gilad, a former associate professor of strategy at Rutgers University's School of Management, and a pioneer in the field of competitive intelligence and war gaming says the only people who consider CI as being industrial espionage "are those who haven't left their caves since Y2K. Today's misconceptions are too sad even for Austin Powers." CI is not spying or snooping but rather a cyclical process of gathering the right information and turning that into strategic insights and intelligence by applying analysis. The confusion with spying comes from the information gathering side – we can assume that not all companies and organisations adhere to sound ethical principles and laws in their quest to lay their hands on sensitive information. Hacking, planting spying devices, stealing information, coercing or blackmailing employees to share sensitive company information and using guises e.g. posing as students or interested members of a trade delegation are all fair techniques in the world of industrial snooping. "All is fair in love and war" as the proverb attributed to John Lyly's Euphues: The Anatomy of Wit goes. CI is unfortunately no exciting as an activity – it is a hard, unglamorous slog. If companies have an effective CI process they need not indulge in spying.[1]

In today's market, staying ahead of your competitors can drastically effect how well your company performs. Knowing a rival's next move and understanding their business strategy has helped corporations form their own business plans. That's why companies need to practice CI, loosely defined as the act of gathering and analysing information about other businesses or industries in a competitive market. Competitive intelligence exists in a grey area between industrial espionage and

ethical information gathering. The difference between having a healthy competitive strategy and unethically spying on other companies is the way in which you collect and process this information. When done effectively, competitive intelligence is simply a way to better understand how your business fits into a specific market. It is a relatively new term for a practice that has been in effect for decades. Every company will have a slightly different view on the term as they mould their business and marketing strategies to fit their needs. Some companies merely track their competitors, while others implement entire multilevel competitive strategies centred on the data they gather.[2]

CI is practiced in a number of ways. Some companies have a single person in marketing monitoring the competitive environment whilst other have larger teams that mine for competitor information and advise the leadership on competitive strategy. A quick search on job listing services LinkedIn unearths dozens of competitive intelligence roles waiting to be filled at big-name firms such as Amazon as well as smaller start-ups. CI activities range from setting up a Google alert for a competitor's name or product counts as doing competitive intelligence; scouring a competitor's job listings (much of what people learned about Apple, Uber and Google's plans for autonomous vehicles came from looking at their job ads) or buying reports from business services companies such as Dun & Bradstreet. Today, in addition to scouring publicly available information, it's not uncommon for companies to buy data from credit card and analytics firms that have aggregated customer information. In fact, entire companies such as Slice Intelligence have built their business around mining and selling user data to third parties.

Back to industrial espionage and snooping: Although the rise of the internet and related technologies has been a boost for companies that want to stay up-to-date on their competition, it has also made it easier for companies to collect information in unethical ways. Trade secret theft and patent infringement cases are abundant in the news, with some involving big corporations like Apple and Samsung. With the recent discovery of Chinese workers hacking into American companies, more people are questioning the morality of competitive research. Hacking into a company's computer system or posing as an employee and stealing information are both obviously unethical practices, but what about other intelligence-gathering initiatives? Where do we draw the line? While it's true that all companies will have a different opinion on the matter, one thing is clear: spying on other corporations does not fall under the umbrella of CI. Many experts believe that companies are beginning to lose sight of what ethical market research is in their drive to get ahead. They put an emphasis on collecting as much data as possible, but don't know what to do with it once they have it. Some companies seek to hurt other businesses through competitive research, rather than using this knowledge to improve their own bottom-line. While such activities might not harm your company in a legal sense, it can hurt your company's reputation in the eyes of the consumer (think pharmaceutical company Aspen Pharma and

Box 1: Examples of modern-day spying

In a January 2010 blog post, Google disclosed that it detected the previous month a highly sophisticated cyberattack originating from China that resulted in the theft of its intellectual property. The company said evidence suggested that a primary goal of the attackers was to access the Gmail accounts of Chinese human rights activists. Google said a wide range of companies were also targeted, including those in the finance, technology, media, and chemical industries. "This is a big espionage program aimed at getting high-tech information and politically sensitive information," James A. Lewis, a cyber and national security expert at the Center for Strategic & International Studies, told the Washington Post.

Hackers stole proprietary information from six U.S. and European energy companies, including Exxon Mobil, Royal Dutch Shell, and BP, according to investigators and one of the companies. McAfee said the attacks resulted in the loss of "project-financing information with regard to oil and gas field bids and operations." It also said the attacks, dubbed Night Dragon, originated "primarily in China" and began in November 2009. Marathon Oil, ConocoPhillips, and Baker Hughes were also hit, according to people familiar with the investigations. Hackers targeted computerized topographical maps worth "millions of dollars" that locate potential oil reserves.

automaker Volkswagen and the damage their corner-cutting has caused the brand). Many unethical information-gathering practices are not illegal, so it is often up to the corporation to decide what is right and wrong. If you find yourself questioning whether or not your company's actions are dishonest, it might be a sign that they are involved in some unethical practices.[3]

SOME REAL-LIFE SITUATIONS

For as long as there has been commerce, there has been espionage (refer boxes 1 and 2). The methods for spying on competitors have changed over time, but the desire to uncover a rival's secrets has not. It is perhaps prudent to realise that while you may choose not to keep an eye on the competitor that does not mean the competitor is not eyeing you. Unwelcome probing is alive and well. And practicing ethical and legal information gathering is a healthy activity. It is about figuring out what the competition is doing: What are they saying to shareholders and the press? What's in their publicly available financial documents? What products have they launched? Yet a fine line is crossed when spying comes into play. Often the play is highly complicated, elaborate, sophisticated and lengthy.

A short news item in USA Today in March 2014 reported that a San Francisco jury found two men guilty of stealing trade secrets from DuPont. It is a story about Walter Liew, an American citizen, born in Malaysia of Chinese parents. His wife is a Chinese citizen. Liew, his wife, and Robert Maegerle, a 78-year-old retired DuPont engineer, were charged with stealing trade secrets from DuPont for producing a chemical, chloride-route titanium dioxide, also known as TiO2. Companies use

Box 2: Examples of modern-day spying

Hewlett-Packard's board became ensnared in a scandal in 2006 after the company spied on its directors, reporters, and employees in a probe to ferret out the source of boardroom news leaks. Investigators hired by the company obtained personal phone records by posing as reporters and company directors. They also trawled through garbage and followed reporters. As a result, then-Chairman Patricia Dunn, who approved the spying, was fired. HP also agreed to pay $14.5 million to settle an investigation by California's attorney general, $6.3 million to settle shareholder lawsuits, and an undisclosed amount to settle a case filed by journalists at the New York Times and Business Week, which is now owned by Bloomberg.

In South Africa, two former police officers who went to work for private corporate investigation companies paid cash to South African law enforcement officials to disrupt a tobacco company's competitors' business operations by falsely suggesting they were marketing and selling cigarettes unlawfully. The aim, often successful, was to get rivals' stock impounded and discourage wholesalers from dealing with rival firms.

In 1993, General Motors accused Volkswagen of industrial espionage after Jose Ignacio Lopez, the chief of production for GM's Opel division, left to join the rival German automaker, along with seven other executives. GM claimed its corporate secrets were used at VW. In the end, the companies agreed to one of the largest settlements of its kind: GM would drop its lawsuits in exchange for VW's pledge to buy $1 billion of GM parts over seven years. In addition, VW was to pay GM $100 million.

TiO2 to whiten a wide variety of products such as cars, paints, metal, paper, plastic, and to whiten the center of Oreo cookies etc. The three was accused of selling the formula to a Chinese competitor of DuPont, Pangang Group. Apparently Pangang paid the couple about US$20 million for the technology. Pangang Group tried to buy the formula from DuPont and was turned down multiple times. China imports a great deal of TiO2 and, according to documents presented in the espionage trial, has declared that getting DuPont's recipe was a national imperative. Liew and his wife founded their company specifically to accomplish that. According to Bloomberg, federal agents found documents in which Liew claimed that a former secretary general of China's state council encouraged him in 1991 to obtain technologies beneficial to the nation, including TiO2. Robert Maegerle, who provided the technical secrets, worked at DuPont.

The New York Times reported in April 2017 that Uber has a Department of Competitive Intelligence which focuses on "studying" its rivals. Uber's Competitive Intelligence team bought anonymized data — including information on Lyft receipts gleaned from customer inboxes — from analytics firm Slice Intelligence. Although both companies faced criticism over their practices (Slice for obtaining the data and Uber for buying it) these action should not be surprising. These are examples of intricate efforts. But they need not always be. A wine producer might do a little incognito investigation into how other wine produc-

ers are faring. She goes into retail shops and wholesale outlets and engages in conversations. One producer said "It's amazing what some people will tell you about their challenges and how their year went".[4]

Look at this headline in the Wall Street Journal:[5]

BUSINESS

U.S. Ups Fight Against Agricultural Espionage

FBI used surveillance tactics authorized by anti-spying law to nab Chinese executive accused of stealing seeds

By Jacob Bunge

April 23, 2015 8:04 a.m. ET

DES MOINES, Iowa—The criminal trial of a Chinese executive accused of stealing high-tech U.S. corn seeds is turning into a battle over the federal government's use of an anti-spying law to fight industrial espionage.

U.S. prosecutors say Mo Hailong, an official with a Chinese agriculture company, participated in a multiyear scheme to pilfer seeds from test fields of U.S. agribusiness giants Monsanto Co. and DuPont Co. The prosecutors claim that Mr. Mo, who was

accenture

BREAKING T

Read the story about the arrival in New York of Igor Sporyshev in 2010 supposedly a trade representative of the Russian Federation. One red flag for the FBI was that his father, Mikhail, had been a KGB officer and a major general in its successor agency, the Federal Security Service (FSB). In 2011, Sporyshev attended a usual energy conference in New York, as did an FBI agent, posing as a Wall Street analyst. The Russian introduced himself, chatted amicably, exchanged business cards, and later followed up. In subsequent conversations, Sporyshev pushed the supposed analyst for information about the energy industry, such as company financial projections and strategy documents. The information was hardly a secret or even sensitive. It did not give

Box 3: Examples of modern-day spying

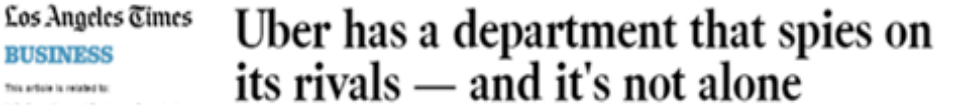
In 1998, when White House national security advisor's security people cleared her Jerusalem hotel suite for bugs and intruders, they might have had in mind a surprise visitor to Vice President Al Gore's room: a spy in an air duct. A Secret Service agent who was enjoying a moment of solitude in Gore's bathroom before the VP arrived heard a metallic scraping sound. The Secret Service had secured Gore's room in advance and they all left except for one agent, who decided to take a visit to the bathroom. The room was all quiet, and he hears a noise in the vent. He sees the vent clips being moved from the inside. And then he sees a guy starting to exit the vent into the room. He kind of coughed and the guy went back into the vents. Newsweek, 5 August 2014.

Sporyshev an edge he could use to commit insider trading. Rather, asking for information like this reflected a Russian approach to intelligence that has endured long after the Cold War. Russian agents tend to prioritise human recruitment and generally discount the huge amount of open source news and information that flows routinely out of the US in government reports, independent news articles, and think tank analyses. “Whispered conversations always feel sexier,” it is said. They cultivate relations and build legends over many years: relationships that start out innocuously, with junior or midlevel workers, can be cultivated over years, until the target is senior and desensitized to sharing information with someone they think of as a long-time friend.

TECHNOLOGY HAS CHANGED THE MO: THE ETHICAL CONSEQUENCES

Technology has certainly raised the bar in the espionage world. Whilst human intelligence remains sexy, the espionage story of the year, and perhaps one of the greatest foreign operations in decades, has undoubtedly been Russia’s effort to influence the 2016 presidential election through hacking penetrating Democratic National Committee servers and the e-mail account of John Podesta, Hillary Clinton’s campaign chairman. The strategy marks an evolution for Russia, which historically has valued so-called human intelligence, over signals intelligence. It is an evolution borne of some necessity, as Russia has in recent years struggled to install spies on American soil. Technology has brought to the table is the ability for companies to drill down deeper into people’s information than anybody ever expected. Many of the rules of the roads on respecting people’s privacy are being rewritten. In the case of Uber and Slice Intelligence, the question on competitive intelligence is going to be how the information was obtained and was there consent of the individual. Using technology, Slice Intelligence-owned Unroll.me, was responsible for scouring people’s inboxes for data, the company has a Privacy Policy that users agree they have read and understand before they even sign up for the service. However Slice does not state clear enough about what the firm did with users’ data. The source of a company’s competitive intelligence is key and said companies that are good at it tend to adopt formal guidelines that ensure they don’t cross legal and ethical lines.

One such guideline is keeping track of where information comes from. Another is ensuring that no terms of use, nondisclosure agreements or privacy policies are violated e.g.


Los Angeles Times
BUSINESS
Uber has a department that spies on its rivals — and it's not alone

using a competitor's service to scope out its prices is fine because the competition probably is expecting it. However paying a product distributor to find out what styles a competing company will be selling next season or what it plans to stock would cross a line because no company would anticipate that its rivals would gain such access. When information gathering goes too far and a company believes that its trade secrets have been stolen, it can lead to lawsuits. Waymo (a self-driving-car company) filed a lawsuit against Uber accusing it of hiring a former Waymo employee who took company files with him.

HOW THEY GATHER INFORMATION

Companies use various ways to gather information and not all are ethical and not all are legal. The legal ones include the following:

- Elicitation: People contracted to gather information often use the Internet to source the names of key persons and contacting them to elicit key information. Various sites could be helpful from sites where disgruntled employees post their gripes to sites that contain trade contact information and Facebook and LinkedIn are good points of departure. They then target such people for information being skilled elicitors. In an interview, in 2013, a corporate spy said sensitive information can be gathered from conversations with people by being an expert in elicitation i.e. People tell you things that can help a business at the expense of another.[6] They do not break the law but they also do not give the background as to why they ask certain questions – they keep the true motivation under wraps. Elicitors are after information that is not in the public domain including sales figures, the revenue a company expects its stores to earn, inventory figures, customer counts, and cash flow. It is also exactly the sort of thing a business needs to understand about its competitors to effectively price and promote a new product.
- Internet searches: Mostly competitor websites, analyst reports, business prospectuses, annual reports, press releases, job advertisements, Dun & Bradstreet reports, court reports and incorporation records serves as a starter. Most of the back-


The Spy Who Added Me on LinkedIn

Russia had operatives in New York for years, from Wall Street to the UN. Now one is headed to prison.

by Garrett M Graff
November 15, 2016, 12:00 PM GMT+2
From BloombergBusinessweek | Subscribe | Reprints

ground secondary research can be conducted with nothing more than an Internet connection and solid research skills.

- Observation e.g. visiting stores, counting cars in the company car park, sitting in reception and observing the activities.
- Analysing the leadership of competitors or newly appointed executives and their actions in previous positions.
- Trade shows and trade visits.

As mentioned, the ways in which people elicit information are numerous and we should be vigilant at all times when we communicate especially where questions arise that might make us feel uncomfortable in answering. Bloomberg Businses week carried an article titles "the Spy Who Added Me on LinkedIn."[7] Rather be vigilant than naïve when dealing with business contacts: The saying goes that in business we have not friends; only interests.


The Telegraph HOME | NEWS | SP

Business

Economy | Companies | Opinion | Markets | Brexit | A-Z | Alex | Telegraph Connect

Business

Inside the murky world of spies for hire

DEFENSIVE MINDSET

What can be done to prevent falling victim to unwelcome snooping and spying:

- Invest in a corporate culture: Defence starts with the relationship between your company and its employees. Human factors are always the weakest link in a security system and that is not true only of computer security. People who feel mistreated by their employer tend to be more willing to discuss that employer's shortcomings, both on the phone and online.
- Institute a sensitising programme: Get experts to regularly sensitise employees about the need to remain vigilant especially when dealing with visitors and delegations and people that ask questions that have an uncomfortable ring to them. Do basic research on people that approach you for information. Beware the invisible phone number and the un-Google-able identity: There might be a reason why people are difficult to google or make No-ID calls. It would be advisable to remain

prudent when dealing with the unknown. And check out the person's background and whether what he / she says is true.

- Clear the company website from too much information and think carefully about what your employees divulge at conferences and workshop and public fora. Websites are often a good source of information for those that want to know more about you.
- LinkedIn, Facebook, and Twitter: You may want to ask your current employees to keep confidential data out of their profiles. Financial and operational detail is often posted in people's LinkedIn profiles and in résumés on Monster or other job boards that should make anyone playing intelligence defence a little uncomfortable.[8]
- Beware of the fact that companies outsource the unsavoury work: Companies at time choose to outsource the spying so as not to be pointed out as engaging in actions that would not be welcomed by shareholders and the public (remember Splice's Uroll.com learning experience) Be aware that there are spies for hire out there.[9]

A few in-house guidelines and examples:

What have to be secured?

- Budgets
- Computer programmes and network information
- Information about Suppliers, Contractors and Clients
- Legal information and advice, minutes, memos and decisions
- Market related issues
- Personal Profiles & addresses of key employees
- Production processes, product development, formulas and specifications
- Remuneration Policy, information and records
- Research and Development programs
- Strategic information and objectives, Business and Marketing Plans
- Stock keeping and levels

Employees

- Ensure that factual information is continuously and correctly communicated to employees through the management line structure.
- Sensitise employees to identify what need to be secured in their own work environment for example information about clients, detail of contractual agreements.

Offices, Premises and Access

- Keep the office tidy, organised and lock office when leaving.
- Maintain strict access control to offices, premises and facilities.
- Visual identification of suppliers, clients, consultants, auditors and other visitors.
- No visitors should be left unattended or unguided.

Telephone and Faxes

- Restrict as far as possible telephone conversations about sensitive issues.
- Be aware of strange calls and requests for information.
- Do not give more information than that which has been requested.
- Be sensitive towards the repair of telephones/fax machines if not requested.
- Faxes are unsafe. Sensitive information should not be sent via fax.

Documentation

- Ensure all confidential, sensitive and classified documents are retrieved from employees on leaving employment.
- When travelling only take the necessary documents.
- Shred confidential, sensitive and classified documents.
- Lock confidential, sensitive and classified documents when not used.
- Deliver where possible confidential, sensitive and classified documents in sealed envelopes by hand.
- Handle the delegation of duplicating confidential and classified documents with sensitivity; restrict number of copies of sensitive documents.

Computers

- Control physical access to personal computers and select passwords carefully.
- Do not leave computers unattended when on.
- Only the addressee should open own e-mail.

Production/Manufacturing

- Safeguard technology, programmes, capacity, knowledge, prototypes, methods, systems and experience.
- Handle visitors with sensitivity and what may be photographed.

Research and Development

- Weigh the free interaction regarding scientific, research and development issues up against safe guarding own assets and intellectual property.
- Verify bona fides and interests of potential business associates.
- Be aware of misleading tactics, disinformation or misrepresentations.

Important Management Issues

- Management is usually top targets due to the fact that they have the most sought after information.
- The presence of outsiders at meetings should be on need-to-know bases.
- Guide secretaries and assistants how to handle sensitive information.
- Apply the need-to-know principle in discussions with outsiders.
- Be aware of shortcomings and vulnerabilities in one's own ego.

Handling requests in a client-friendly way

- Ask for what reason the information is requested. [Why?]
- Ask exactly which information is required. [What?]
- Ask detail contact particulars. [Who?]
- When uncertain undertake to discuss the request with your superior and promise to give feedback.

Remember there is a line that should not be overstepped: i.e. the line between gathering overt information using various techniques as mentioned and spying or industrial espionage. That is a next level type of action bugging and stealing and snooping. You do not want your unsuspecting employees being unwittingly debriefed by skilled elicitors out to find out what your company's financials are. Perhaps it is opportune to look at the foreign interns and summer employees in a different light ... what if they report back to e.g. a French DGSE officer? It's not improbable.

CONCLUSION

Like any other industry, the wine industry is no immune or safe from competitor probing. Visiting delegations, visiting students and interns, trade shows and other could all potentially provide opportunities to slip in an ostensibly innocuous question. There are players that are pro-active and that have taken measures to mitigate risk and limit data leaks. The reason being that intellectual property should be protected against both carelessness and malicious intent.[10] [11] It happens all the time and often we are unwitting observers and participants. We should rather err on the side of vigilance and play for time and not feel that we should part with sensitive and proprietary information.

ENDNOTES

1 *http://www.competing.com/2014/04/first-conviction-ever-under-the-1996-espionage-act/*
2 *http://www.competing.com/2014/04/first-conviction-ever-under-the-1996-espionage-act/*
3 *http://lauthinvestigations.com/blog/2014/05/competitive_intelligence/*
4 *In Vino Veritas, 2010. JM Gregson. Severn House Publishers Ltd, 01 Mar 2012*
5 *https://www.wsj.com/articles/u-s-ups-fight-against-agricultural-espionage-1429790642*
6 *https://www.inc.com/magazine/201302/george-chidi/confessions-of-a-corporate-spy.html*
7 *https://www.bloomberg.com/news/articles/2016-11-15/the-spy-who-added-me-on-linkedin*
8 *https://www.inc.com/magazine/201302/george-chidi/confessions-of-a-corporate-spy.html*
9 *http://www.telegraph.co.uk/business/2017/01/28/bond-broadband-back-business-spying-coming-full-circle/*
10 *https://www.mimecast.com/resources/press-releases/dates/2010/12/dgb-keeps-email-flowing-with-mimecast/*
11 *http://www.latimes.com/business/la-fi-tn-competitive-intelligence-20170427-htmlstory.html*

Compiled, in collaboration with SAWIS, by
Dr Marie-Luce Kühn, IBIS Business and Information Services (Pty) Ltd
PO Box 7048, Stellenbosch 7599
Tel +27 21 883 2855
e-mail: mlm@ibis.co.za website: www.ibis.co.za

A SAWIS Publication.

ibis™
strategic environmental analysis