Israeli Spy Companies: *Verint and Narus*

By Richard Sanders

In the mid-2000s, two Israeli spy companies (Narus and Verint) were caught in the centre of a huge scandal involving the wiretapping of virtually all US phone and internet messages. Their mass surveillance services were used by America's two largest telecom companies, AT&T and Verizon. (See AT&T pp.7-8, and Verizon in table, "CPP Investments," p.53.)

These telecom giants, which together control 80% of the US market, were turning over all of their customers' internet communications and phone call records to the US National Security Agency (NSA). On hundreds of occasions, these data transfers were done without legal warrants or court orders. This warrantless wiretapping operation was a gargantuan task requiring the collection, analysis and transfer of data relating to billions of messages per day. To accomplish this, AT&T employed the services of an Israeli spy firm called Narus, while Verizon used a different Israeli spy company, Verint Systems.

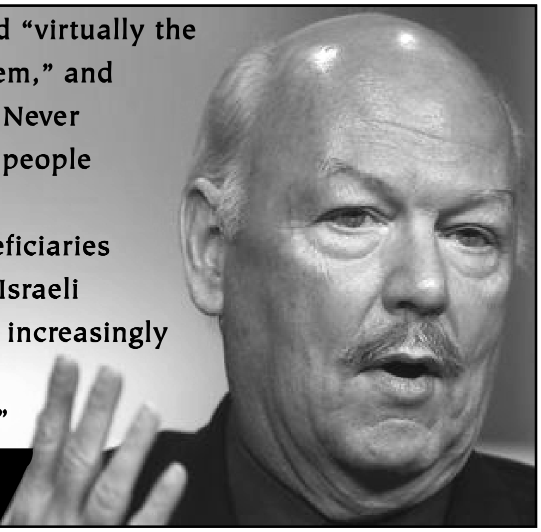
The technologies of both Verint and Narus have also been absorbed into the spy products of other companies. For example, Amdocs has integrated Narus software into its products, while Verisign has incorporated systems from both Verint and Narus into its "NetDiscovery" service. (See Amdocs, pp.5-6, and Verisign in table "CPP Investments," p.53.)

James Bamford, a former ABC News director and journalist who has researched intelligence agencies for three decades, has reported that:

> "Verint and Narus are super-intrusive – conducting mass surveillance on both international and domestic [US] communications 24/7. What is especially troubling, but little known, is that both companies have extensive ties to a foreign country, Israel, as well as links to that country's intelligence service – a service with a long history of aggressive spying against the U.S."

A glimpse into this "long history" of Israeli intelligence agencies targeting the US is discussed by Philip Giraldi, a former CIA counter-terrorism specialist and military-intelligence officer who served 19 years in Turkey, Italy, Germany, and Spain. He notes that Israel "always features prominently" in the FBI's annual report, "Foreign Economic Collection and Industrial Espionage." Its 2005 report, he says, stated:

> "'Israel has an active program to gather proprietary information within the US. These collection activities are primarily directed at obtaining information on military systems and advanced computing applications that can be used in Israel's sizable armaments industry.' It adds that Israel recruits spies, uses electronic methods, and carries out computer intrusion to gain the information.
>
> "In 1996…the Pentagon's Defense Investigative Service warned [US] defense contractors that Israel had 'espionage intentions and capabilities' here [in the US] and was aggressively trying to steal military and intelligence secrets. It also cited a security threat posed by individuals who have 'strong ethnic ties' to Israel, stating that 'Placing Israeli nationals in key industries … is a technique utilized with great success.'"



Verint and Narus have bugged "virtually the entire American telecom system," and "wired much of the planet.... Never before in history have so few people wiretapped so many."

"[T]he greatest potential beneficiaries of this marriage between the Israeli eavesdroppers and America's increasingly centralized telecom grid, are Israel's intelligence agencies."

James Bamford, author of *The Shadow Factory*

Giraldi says that when the General Accounting Office (GAO), the investigative arm of Congress, researched spying against US arms industries in 1996, it said Israel "conducts the most aggressive espionage operation against the US of any U.S. ally." The GAO also reported that

> "Israeli citizens residing in the U.S. had stolen sensitive technology to manufacture artillery gun tubes, obtained classified plans for a reconnaissance system, and passed sensitive aerospace designs to unauthorized users. An Israeli company was caught monitoring a Department of Defense telecommunications system to obtain classified information."

Another ex-CIA officer who expressed grave concerns about Israel's spying is Robert David Steele. He said "Israeli penetration of the entire US telecommunications system means that NSA's warrantless wiretapping actually means Israeli warrantless wiretapping."

Jane's Intelligence Group reported in 2004 that Israeli intelligence agencies "have been spying on the U.S. and running clandestine operations since Israel was established."

In 2008, Harry Brandon, a former FBI deputy director of counterintelligence told *Congressional Quarterly* (*CQ*) magazine that "the Israelis are interested in commercial as much as military secrets." *CQ* surmised that "One effective espionage tool is forming joint partnerships with U.S. companies to supply software and other technology products to U.S. government agencies." This is precisely what Verint and Narus have done so effectively.

But, as Bamford points out, Verint and Narus haven't just bugged "virtually the entire American telecom system," these "two firms…have also wired much of the planet…. Never before in history have so few people wiretapped so many."

COMVERSE
VERINT
POWERING ACTIONABLE INTELLIGENCE

Verint Systems Inc.

Verint is a subsidiary of Comverse Technology which is "the world's leading provider of …communications intercept and analysis" technology. Founded in Israel and with half its employees based there, Verint's parent company has attracted its fair share of people from Israel's military and intelligence communities.

A search of the *Business News* website finds the "Executive Profiles" of about twenty key Comverse people who had worked for Israel's military. Of these, at least six were in Israeli intelligence. For example, Alon Geva was "an officer at the elite Intelligence unit of the Israeli Defense Forces," Yoav Shaked "started his career as an officer in the Israeli Defense Force [IDF] Intelligence Corps," Chaim Bechor "served as a technical officer in the Intelligence Corps of the IDF," Uri Kolodny "served over 4 years in …Israeli Intelligence," Alon J. Bender was the "Senior Security Technology consultant on several Israeli government projects (Prime Minister's Office, IDF and Secret Intelligence), and Noam Livnat "served four and a half years in the Israeli Defense Forces' prestigious Intelligence Corps 'Talpiyot' project."

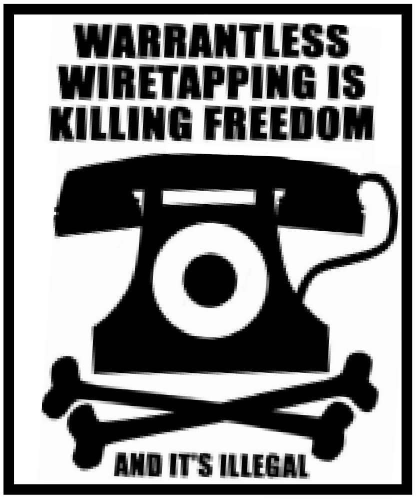
Originally called Comverse Infosys, Verint makes electronic systems to monitor, collect and analyse voice, email and video communications. In reference to Verint's role in this trade, Bamford notes that by 2004:

> "a large percentage of America's – and the world's – voice and data communications were passing through wiretaps built, installed, and maintained by a small, secretive Israeli company run by former Israeli military and intelligence officers."

Verint says its customers include "85 percent of the Fortune 100." They use the company's products, Verint says, "to improve enterprise performance and make the world a safer place." Although secretive about its clients, the Verint website divulges a few. Among them are several corporate giants that support Israel's military, namely, Cisco, Hewlett Packard (HP), Honeywell, Siemens and EMC. (See p.19, p.36 and pp.39-40. For Siemens and EMC, see table, "CPP Investments," p.53.)

But besides serving big business, Verint also sells spyware to "law enforcement, national security, intelligence, and other government agencies." Its technology was used by US telecom giant Verizon to fulfil the mass surveillance requests – legal and otherwise – from the NSA. "[T]he greatest potential beneficiaries of this marriage between the Israeli eavesdroppers and America's increasingly centralized telecom grid," says Bamford, "are Israel's intelligence agencies."

Besides the US, Verint's other major government clients include Mexico, Vietnam, Australia and the Netherlands. Government users in the two latter countries have raised grave concerns about the security of Verint's products and particularly their remote control from Israel. For instance, Christopher Ketcham reported that:



> "In November 2002, sources in the Dutch counterintelligence community began airing what they claimed was 'strong evidence that the Israeli secret service has uncontrolled access to confidential tapping data collected by the Dutch police and intelligence services.'"

In 2003, a Dutch technology magazine, *c't*, ran an article, "Dutch Tapping Room not Kosher." It said "[a]ll tapping equipment of the Dutch intelligence services and half the tapping equipment of the national police force…is insecure and is leaking information to Israel." The leaky technology was T2S2 tapware "delivered to the [Dutch] government in the last few years by the Israeli company Verint."

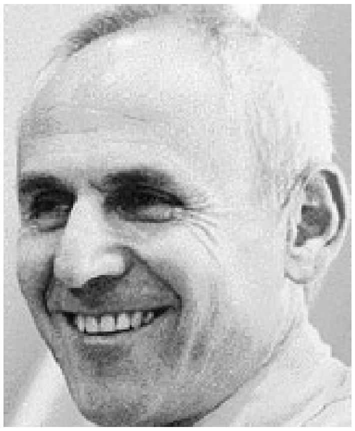
Verint's cofounder, Jacob "Kobi" Alexander, chaired its board from 1994 until 2006 when he fled to Israel and then Namibia to evade 36 charges of conspiracy, fraud and money laundering.

In 2004, Verint's mass surveillance systems were called "a lemon" in the Australian media and a parliamentary committee monitoring the government's Corruption and Crime Commission (CCC) summoned Verint executives to a "closed session." The committee told Verint that they had "some issues" with the "data interception" systems being used by "at least six different law enforcement agencies across Australia." The MPs said their "issues" with Verint included that it "can access data from overseas but the CCC seems restricted in its ability to access data." Verint's Tel Aviv-based representative confirmed: "We sometimes operate by remote access."

Bamford has called it "unnerving" "that Verint can automatically access the mega-terabytes of stored and real-time data secretly and remotely from anywhere, including Israel."

Verint's board of directors has always included former military and intelligence officers from the US and Israel. The most infamous of these is Jacob "Kobi" Alexander, an Israeli entrepreneur who cofounded both Comverse and its off-shoot, Verint. Alexander is a former Israeli intelligence officer who chaired Verint's board from its creation in 1994 until 2006, when he was indicted in the US on 36 charges of conspiracy, fraud and money laundering. Leaving the boards of Verint and Comverse, Alexander evaded US prosecution by going to Israel. Placed on the FBI's "Most Wanted List," Verint's disgraced cofounder was eventually arrested (and held very briefly) in Namibia, where he is still fighting extradition. Despite this, Alexander's current "Executive Profile" on *Business Week*'s website says he has been a Comverse "Advisor" "since May 1, 2006."

Another former Verint board member with a Israeli intelligence background is Ronen Nir. Before joining Verint's board, and becoming vice president of its Analytics and Communications Solutions Division, Nir served 13 years in "the Israeli Defense Forces' elite Intelligence unit." Nir remains a Lieutenant Colonel in Israel's military reserve forces.



Carmel Vernia was Chief Operating Officer of Comverse and CEO of Verint. Then, as Israel's top government scientist, he oversaw the grant program that reimbursed up to 50% of Comverse's R&D expenses. Later, he joined the board of Verint spin off, PerSay. Its products search for and identify specific speakers in the vast sea of intercepted messages.

Other Verint directors have links to US intelligence agencies and the military industrial complex. For example, US Lieutenant General Kenneth Minihan joined Verint's board in 2002. Since the Vietnam war, this 30-year veteran of the US Air Force held many top military intelligence postings. His career culminated in leading the Defense Intelligence Agency (1995-1996), the National Security Agency and the Central Security Service (1996-1999).

Two other US military veterans on Verint's board are Larry Myers and Victor De Marines. Both have longstanding links to MITRE Corp., which provides computer security for the US military and intelligence agencies. De Marines managed MITRE's Center for Integrated Intelligence Systems and oversaw its Intelligence and Electronic Warfare Systems. While managing MITRE's office in Bangkok, Thailand (1967-1969), he "helped coordinate MITRE's support for [US] Air Force systems ...on support operations." DeMarines still serves on an advisory group for the National Reconnaissance Office, a US intelligence agency that operates the CIA's spy satellites.

Dan Bodner, who has been Verint's president and CEO since 1994, was an army engineer in Israel's Defense Forces. Another Verint director, Meir Sperling, held executive positions in two Israeli telecom companies, Tadiran and ECI, which both serve police and military agencies around the world, including Israel's armed forces.

Verint's ties to Israel's government are personified in Carmel Vernia, who started at Comverse in 1984 and was its Chief Operating Officer between 1994 and 2000. He became the first Verint CEO in 1999 but was soon appointed by Israel's government to become the Ministry of Industry and Trade's Chief Scientist. His responsibilities included overseeing the annual distribution of about US$450 million in R&D grants to Israel high-tech companies, including Comverse.

A 2001 Comverse document states that "we continue to receive significant benefits through reimbursement of up to 50% of qualified research and development expenditures" through a "grant program administered by the Office of the Chief Scientist of the Ministry of Industry and Trade."

After leaving his post as Israel's Chief Scientist in 2002, Vernia became a director of PerSay, an Israeli company that spun off from Verint in 2000. It received early funding from Poalim Investments, a subsidiary of Bank Hapoalim. (See pp.10-11.) PerSay's speaker recognition technology includes voice biometrics systems that search for and identify individual speakers within the vast sea of intercepted phone calls. Bamford notes that

> "PerSay is an example of how close and interconnected these companies are with Israel's intelligence community – a factor of great concern considering how much of their bugging equipment is now secretly hardwired into the American telecommunications system."

Bamford goes on to say that PerSay's board included Arik Nir,

> "a former senior official in Shin Bet, Israel's internal security service. Nir is also the managing director of PerSay's financial backer, Athlone Global Security, which counts former Mossad chief Ephraim Halevy on its advisory board."

Business Week's website shows that Halevy also sits on the board of Israel's Makhteshim Agan, an explosives-making subsidiary of one of Israel's largest holding companies, the Discount Investment Corp. (See p.25.)

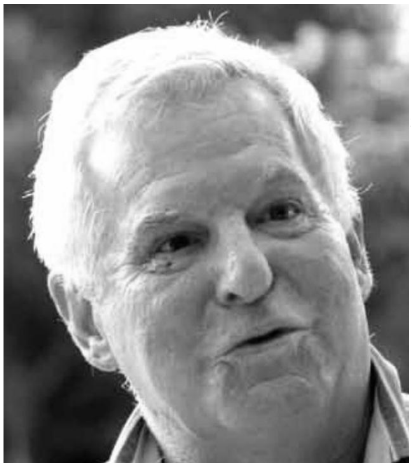
In writing about Verint and PerSay, Bamford has noted that

> "With remote access to the internal and international voice and data communications of over one hundred countries around the world, including the United States, Verint's headquarters in Tel Aviv has a capacity rivaled only by NSA's, if not greater, especially when coupled with PerSay's voice-mining capability."

In 2004, Verint paid US$35 million for the "government surveillance business" of Israel's ECtel Ltd. Verint said this would give it "additional communications interception capabilities for the mass collection and analysis of voice and data communications."

Yair Cohen, became ECtel's chair in 2006. For the five previous years, Cohen led Israel's equivalent of the US National Security Agency. *Business Week*'s online biography says "as Brigadier General of the special unit 8200, the central military intelligence unit of the Israeli Defense Force," Cohen was responsible for "developing state-of-the-art technology and one of the largest, most complex technology organizations in Israel." Cohen was also a director of IDB Group, which controls Discount Investment Corp., and Vice President of one of its prized holdings, Elron Electronics.

In 2011, Verint acquired an Israeli firm called Rontal Applications Ltd. which provides governments and businesses with "physical security information management solutions." The board of this Verint subsidiary has in-



Amiram Levin
In 2011, Verint acquired Rontal Applications, an Israeli militay firm whose board has included retired Major General Levin, a former deputy director of the Mossad.

cluded Israeli Major General Amiram Levin. During his 35-year military career, he was the deputy director of Israel's foreign intelligence agency, the Mossad (1998-2000).

Business News online says Levin held "senior command positions in Special Ops and in the Tank Corps – culminating in the post of Israel's Northern Front Commander." He had "weapon system development duties" and led "strategic weapon development task-forces comprising of military designers & major Israeli defense contractors." Levin also Commanded "Sayeret Matkal," Israel's "elite intelligence and counter-terrorism commando unit."

Upon leaving the military, Levin entered the private sector and joined the boards of several Israeli companies serving the country's military and intelligence agencies. Besides serving with Verint's subsidiary, Rontal, Levin also joined the advisory board of Suspect Detection Systems (SDS) Ltd. This Israeli company says its "anti-terror and anti-crime technology...detects the hidden 'hostile intent' of assailants-before they commit their intended acts." The SDS website says Levin "brings with him extensive support from his many years of experience in interrogation and counter-terrorism." Levin also serves on the advisory board of an Israeli "homeland security" company called Camero Inc. which supplies police and special forces with technology that sees through walls.

Narus Inc.

The name Narus is aptly derived from the Latin word "gnarus" for "all knowing." Calling itself "the leader in real-time traffic intelligence for the protection and management of large [Internet Protocol] IP networks," Narus makes "Semantic Traffic Analysis" software, which "captures comprehensive customer usage data." It also makes "Deep Packet Inspection" systems for "tracking and targeting" email and mobile-phone communications.

In 2005, computer engineer Mark Klein blew the whistle on AT&T, where he had worked for 22 years. Klein then became central to a class-action lawsuit by the Electronic Frontier Foundation. The lawsuit exposed evidence that AT&T had transferred vast amounts of data to the NSA using a Narus supercomputer called the STA 6400. Klein testified that:

> "In 2003 AT&T built 'secret rooms' hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire Internet. These installations enable the government to look at every individual message on the Internet and analyze exactly what people are doing."

The law suit ended in 2009 when the US government granted retroactive immunity to itself and the telecom companies for their roles in the warrantless wiretapping operations.

Narus systems are also used by police and intelligence agencies around the world, as well as by huge internet companies that hand over their customer's data to these agencies. Narus says its systems can "immediately detect, analyze, mitigate and target any unwanted, unwarranted or malicious traffic." However, deciding exactly what constitutes "unwanted" internet traffic is a matter for Narus' customers to decide. This is troubling because besides supplying its wares to the largest telecom providers in the US, Narus systems for monitoring, analyzing and controlling people's everyday use of the internet are also employed by telecom authorities in Egypt, Pakistan, Libya, Saudi Arabia, China and elsewhere.

Mark Klein
This whistleblower revealed that AT&T used Israel's Narus technology "to look at every individual message on the Internet and analyze exactly what people are doing."

So, for example, when widespread calls for democracy and an end to state-sponsored torture and terror were fuelling the "Arab Spring" protests in Egypt, Narus systems were used to close down much of the internet there. In this way, Egypt's US-backed military dictatorship benefited from Narus, an Israeli spy company.

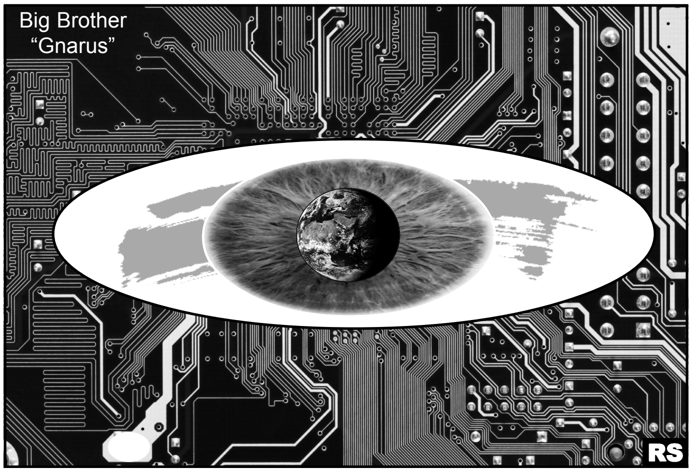
Narus, says the Israeli newspaper *Haaretz*, "was founded in 1997 by Dr Ori Cohen, Stas Khirman and four other guys in Israel." Its initial funding came from an Israeli venture capital fund, Walden Ventures, which has also funded Israeli "homeland security" firms like Camero.

Before starting Narus, its key founders had all worked for VDOnet, an Israeli firm that pioneered internet video streaming. Khirman, who was Narus' Chief Technical Officer, began his high-tech career at Israel Aerospace Industries. (See "State-owned Israeli War Industries," pp.48.) He and other Narus cofounders, have since gone to work for other Israeli high-tech firms. For example, Oren Ariel became the general manager and director of Hewlett-Packard (HP) Labs Israel, whose parent company is a major Israel military contractor. (See HP, pp.36-37.)

Narus has extremely close connections to US military and spy agencies. William Crowell, who has been on Narus' board since 2004, was deputy director of operations before becoming deputy director of the NSA between 1994 and 1997. Since 2007, Crowell has chaired the Senior Advisory Group for the US Director of National Intelligence, who is the principal advisor on intelligence matters to the US President, the National Security Council and the Homeland Security Council.

Another Narus board member is Peter Kersten a "decorated Marine Corps veteran with combat duty in Kuwait and Somalia." Before joining Narus he "managed high-level relationships" between military contractors, the NSA and the Pentagon. Illustrating the value placed by Narus on good relations with US military and intelligence agencies, Kersten is now the its vice president of US Federal Sales.

Further demonstrating this company's integration into the US-led, global military-industrial complex, is Boeing's purchased of Narus in 2010. With US$30.9 billion in military revenues, Boeing is the world's fourth largest war industry, and the premiere manufacturer of warplanes.



References

James Bamford, "The Shadow Factory, the Ultra-Secret NSA from 9/11 to the Eavesdropping on America"
www.grossolatos.com/blog/wp-content/uploads/2011/06/The-Shadow-Factory.pdf

Philip Giraldi, "The Spy Who Loves Us," *American Conservative*, June 2, 2008.
www.theamericanconservative.com/article/2008/jun/02/00006/

Christopher Ketcham, "An Israeli Trojan Horse: How Israeli Backdoor Technology Penetrated the U.S. Government's Telecom System and Compromised National Security," *CounterPunch*, September 27, 2008.
www.counterpunch.org/ketcham09272008.html

Verint Systems, Wikipedia
en.wikipedia.org/wiki/Verint_Systems

Ciara Linnane,"Security-technology rally tied to terror scare," *MarketWatch*, August 10, 2006.
www.marketwatch.com/story/security-technology-shares-rally-on-terror-scare

Alon Geva
investing.businessweek.com/research/stocks/private/person.asp?personId=430653

Yoav Shaked
investing.businessweek.com/research/stocks/private/person.asp?personId=1546234

Chaim Bechor
investing.businessweek.com/research/stocks/people/person.asp?personId=30420383

Uri Kolodny
investing.businessweek.com/research/stocks/private/person.asp?personId=628556

Alon J. Bender
investing.businessweek.com/research/stocks/private/person.asp?personId=6386264

Noam Livnat
investing.businessweek.com/research/stocks/private/person.asp?personId=49648761

Comverse Infosys documents
cryptome.org/verint-spysys.htm

Verint Fact Sheet, July 2010.
verint.com/corporate/misc/file/Verint%20Fact%20Sheet%20July%202010.pdf

Communications Intelligence and Investigative Solutions
verint.com/communications_interception/index.cfm

"America's Israeli Spying Problems," March 10, 2009.
www.billslinksandmore.com/Billsblog/2009/03/10/americas-israeli-spying-problems/

Kobi Alexander
investing.businessweek.com/research/stocks/people/person.asp?personId=263005

Ronen Nir
investing.businessweek.com/research/stocks/private/person.asp?personId=44762727

Kenneth Minihan
investing.businessweek.com/research/stocks/private/person.asp?personId=1908593

Larry Myers
investing.businessweek.com/research/stocks/people/person.asp?personId=8113535

Victor De Marines
investing.businessweek.com/research/stocks/private/person.asp?personId=2201309

Victor Demarines
www.walkersresearch.com/profilePages/Show_Executive_Title/Executive_detail.asp?id=10002658400019

Dan Bodner
investing.businessweek.com/research/stocks/people/person.asp?personId=263013

Meir Sperling
investing.businessweek.com/research/stocks/people/person.asp?personId=268012

Customer Solutions
www.tadirantele.com/tadiran-telecom/customers/government.aspx

IDF Military contractor awarded record $800 million deal with BT, July 9, 2010.
www.inminds.com/article.php?id=10445

Officers/Directors for Israel Growth Partners Ac
167.76.159.8:8020/aa/raweb/fundamp/officer/IGPAU.HTML

Carmel Vernia
investing.businessweek.com/research/stocks/people/person.asp?personId=5646682

Prospectus - Comverse Technology Inc/NY, May 1, 2001.
www.docstoc.com/docs/21682868/Prospectus—COMVERSE-TECHNOLOGY-INCNY—5-1-2001

Yiar Cohen
investing.businessweek.com/research/stocks/people/person.asp?personId=25333492

Rontal Applications Ltd
investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=36311819

Amiram Levin
investing.businessweek.com/research/stocks/private/person.asp?personId=37824298

Major General (Res.) Amiram Levin, Former Deputy Mossad Chief, Joins Suspect Detection Systems' Advisory Board, May 11, 2009.
www.reuters.com/article/2009/05/11/idUS102711+11-May-2009+PRN 20090511

SDS Team
www.suspectdetection.com/team.html

Marc Perelman, "Debate Flares Over Israel's Access to American Secrets," *Jewish Daily Forward*, October 23, 2008.
www.forward.com/articles/14433/

Narus
en.wikipedia.org/wiki/Narus_(company)

Mark Klein, "AT&T Deploys Government Spy Gear on WorldNet Network," January 16, 2004.
scriptkitchen.com/att_klein_wired.pdf

James Bamford, The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America, 2008.
www.grossolatos.com/blog/wp-content/uploads/2011/06/The-Shadow-Factory.pdf

Raphael Fogel, "Ori Cohen, private eye," *Haaretz*, July 11, 2006.
www.haaretz.com/news/ori-cohen-private-eye-1.192771

Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," *Huffington Pos*t, January 28, 2011.
www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html

Raphael Fogel, "Ori Cohen, private eye," *Haaretz*, July 11, 2006.
www.haaretz.com/news/ori-cohen-private-eye-1.192771

Ori Cohen
www.linkedin.com/pub/ori-cohen/0/16/708

Stas Khirman
www.linkedin.com/in/khirman

Oren Ariel
il.linkedin.com/in/oariel

William P. Crowell
investing.businessweek.com/research/stocks/private/person.asp?personId=347467

Peter Kersten
investing.businessweek.com/research/stocks/private/person.asp?personId=22783275