Since the late 1990s, federal agents have reported systemic communications security breaches at the Department of Justice, FBI, DEA, the State Department, and the White House. Several of the alleged breaches, these agents say, can be traced to two hi-tech communications companies, Verint Inc. (formerly Comverse Infosys), and Amdocs Ltd., that respectively provide major wiretap and phone billing/record-keeping software contracts for the U.S. government.

Together, Verint and Amdocs form part of the backbone of the government's domestic intelligence surveillance technology. Both companies are based in Israel – having arisen to prominence from that country's cornering of the information technology market – and are heavily funded by the Israeli government, with connections to the Israeli military and Israeli intelligence (both companies have a long history of board memberships dominated by current and former Israeli military and intelligence officers). Verint is considered the world leader in "electronic interception" and hence an ideal private sector candidate for wiretap outsourcing. Amdocs is the world's largest billing service for telecommunications, with some $2.8 billion in revenues in 2007, offices worldwide, and clients that include the top 25 phone companies in the United States that together handle 90 percent of all call traffic among U.S. residents. The companies' operations, sources suggest, have been infiltrated by freelance spies exploiting encrypted trapdoors in Verint/Amdocs technology and gathering data on Americans for transfer to Israeli intelligence and other willing customers (particularly organized crime). "The fact of the vulnerability of our telecom backbone is indisputable," says a high level U.S. intelligence officer who has monitored the fears among federal agents. "How it came to pass, why nothing has been done, who has done what – these are the incendiary questions." If the allegations are true, the electronic communications gathered up by the NSA and other U.S. intelligence agencies might be falling into the hands of a foreign government. Reviewing the available evidence, Robert David Steele, a former CIA case officer and today one of the foremost international proponents for "public intelligence in the public interest," tells me that "Israeli penetration of the entire US telecommunications system means that NSA's warrantless wiretapping actually means Israeli warrantless wiretapping."

As early as 1999, the National Security Agency issued a warning that records of U.S. government telephone calls were ending up in foreign hands – Israel's, in particular. In 2002, assistant U.S. Attorney General Robert F. Diegelman issued an eyes only memo on the matter to the chief information technology (IT) officers at the Department of Justice. IT officers oversee everything from the kind of cell phones agents carry to the wiretap equipment they use in the field; their defining purpose is secure communications. Diegelman's memo was a reiteration, with overtones of reprimand, of a new IT policy instituted a year earlier, in July 2001, in an internal Justice order titled "2640.2D Information Technology Security." Order 2640.2D stated that "Foreign Nationals shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems." This might not seem much to blink at in the post-9/11 intel and security overhaul. Yet 2640.2D was issued a full two months before the Sept. 11 attacks. What group or groups of foreign nationals had close access to IT systems at the Department of Justice? Israelis, according to officials in law enforcement. One former Justice Department computer crimes prosecutor tells me, speaking on background, "I've heard that the Israelis can listen in to our calls."

Retired CIA counterterrorism and counterintelligence officer Philip Giraldi says this is par for the course in the history of Israeli penetrations in the U.S. He notes that Israel always features prominently in the annual FBI report called "Foreign Economic Collection and Industrial Espionage" – Israel is second only to China in stealing U.S. business secrets. The 2005 FBI report states, for example, "Israel has an active program to gather proprietary information within the United States. 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." A key Israeli method, warns the FBI report, is computer intrusion.

In the big picture of U.S. government spying on Americans, the story ties into 1994 legislation called the Communications Assistance for Law Enforcement Act, or CALEA, which effected a sea-change in methods of electronic surveillance. Gone are the days when wiretaps were conducted through on-site tinkering with copper switches. CALEA mandated sweeping new powers of surveillance for the digital age, by linking remote computers into the routers and hubs of telecom firms – a spyware apparatus linked in real-time, all the time, to American telephones and modems. CALEA made spy equipment an inextricable ligature in our telephonic life. Top officials at the FBI pushed for the legislation, claiming it would improve security, but many field agents have spoken up to complain that CALEA has done exactly the opposite. The data-mining techniques employed by NSA in its wiretapping exploits could not have succeeded without the technology mandated by CALEA. It could be argued that CALEA is the hidden heart of the NSA wiretap scandal.

THE VERINT CONNECTION

According to former CIA officer Giraldi and other US intelligence sources, software manufactured and maintained by Verint, Inc. handles most of American law enforcement's wiretaps. Says Giraldi: "Phone calls are intercepted, recorded, and transmitted to U.S. investigators by Verint, which claims that it has to be 'hands on' with its equipment to maintain the system." Giraldi also notes Verint is reimbursed for up to 50 percent of its R&D costs by the Israeli Ministry of Industry and Trade. According to Giraldi, the extent of the use of Verint technology "is considered classified," but sources have spoken out and told Giraldi they are worried about the security of Verint wiretap systems. The key concern, says Giraldi, is the issue of a "trojan" embedded in the software.

A trojan in information security hardware/software is a backdoor that can be accessed remotely by parties who normally would not have access to the secure system. Allegations of massive trojan spying have rocked the Israeli business community in recent years. An AP article in 2005 noted, "Top Israeli blue chip companies…are suspected of using illicit surveillance software to steal information from their rivals and enemies." Over 40 companies have come under scrutiny. "It is the largest cybercrime case in Israeli history," Boaz Guttmann, a veteran cybercrimes investigator with the Israeli national police, tells me. "Trojan horse espionage is part of the way of life of companies in Israel. It's a culture of spying."

This is of course the culture on which the U.S. depends for much of its secure software for data encryption and telephonic security. "There's been a lot discussion of how much we should trust security products by Israeli telecom firms," says Philip Zimmerman, one of the legendary pioneers of encryption technology (Zimmerman invented the cryptographic and privacy authentication system known as Pretty Good Privacy, or PGP, now one of the basic modern standards for communications encryption). "Generally speaking, I wouldn't trust stuff made overseas for data security," says Zimmerman. "A guy at NSA InfoSec" – the information security division of the National Security Agency – "once told me, 'Foreign-made crypto is our nightmare.' But to be fair, as our domestic electronics industry becomes weaker and weaker, foreign-made becomes inevitable." Look at where the expertise is, Zimmerman adds: Among the ranks of the International Association for Cryptological Research, which meets annually, there is a higher percentage of Israelis than any other nationality. The Israeli-run Verint is today the provider of telecom interception systems deployed in over 50 countries.

Carl Cameron, chief politics correspondent at Fox News Channel, is one of the few reporters to look into federal agents' deepening distress over possible trojans embedded in Verint technology. In a wide-ranging four-part investigation into Israeli-linked espionage that aired in December 2001, Cameron made a number of startling discoveries regarding Verint, then known as Comverse Infosys. Sources told Cameron that "while various FBI inquiries into Comverse have been conducted over the years," the inquiries had "been halted before the actual equipment has ever been thoroughly tested for leaks." Cameron also noted a 1999 internal FCC document indicating that "several government agencies expressed deep concerns that too many unauthorized non-law enforcement personnel can access the wiretap system." Much of this access was facilitated through "remote maintenance."

Immediately following the Cameron report, Comverse Infosys changed its name to Verint, saying the company was "maturing." (The company issued no response to Cameron's allegations, nor did it threaten a lawsuit.) Meanwhile, security officers at DEA, an adjunct of the Justice Department, began examining the agency's own relationship with Comverse/Verint. In 1997, DEA transformed its wiretap infrastructure with the $25 million procurement from Comverse/Verint of a technology called "T2S2" – "translation and transcription support services" – with Comverse/Verint contracted to provide the hardware and software, plus "support services, training, upgrades, enhancements and options throughout the life of the contract," according to the "contracts and acquisitions" notice posted on the DEA's website. This was unprecedented. Prior to 1997, DEA staff used equipment that was developed and maintained in-house.

But now Cameron's report raised some ugly questions of vulnerability in T2S2.

The director of security programs at DEA, Heidi Raffanello, was rattled enough to issue an internal communiqué on the matter, dated Dec. 18, 2001, four days after the final installment in the Cameron series. Referencing the Fox News report, she worried that "Comverse remote maintenance" was "not addressed in the C&A [contracts and acquisitions] process." She also cited the concerns in Justice Department order 2640.2D, and noted that the "Administrator" – meaning then DEA head Asa Hutchinson – had been briefed. Then there was this stunner: "It remains unclear if Comverse personnel are security cleared, and if so, who are they and what type of clearances are on record….Bottom line we should have caught it." On its face, the Raffanello memo is a frightening glimpse into a bureaucracy caught with its pants down.

American law enforcement was not alone in suspecting T2S2 equipment purchased from Comverse/Verint. 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,” according to the Dutch broadcast radio station Evangelische Omroep (EO). In January 2003, the respected Dutch technology and computing magazine, c’t, ran a follow-up to the EO scoop, headlined “Dutch Tapping Room not Kosher.” The article began: “All 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 writer, Paul Wouters, goes on to discuss the T2S2 tap-ware “delivered to the government in the last few years by the Israeli company Verint,” and quoted several cryptography experts on the viability of remote monitoring of encrypted “blackbox” data. Wouters writes of this “blackbox cryptography”:

> …a very important part of strong cryptography is a good random source. Without a proper random generator, or worse, with an intentionally crippled random generator, the resulting ciphertext becomes trivial to break. If there is one single unknown chip involved with the random generation, such as a hardware accelerator chip, all bets are off….If you can trust the hardware and you have access to the source code, then it should theoretically be possible to verify the system. This, however, can just not be done without the source code.

Yet, as Wouters was careful to add, “when the equipment was bought from the Israelis, it was agreed that no one except [Verint] personnel was authorized to touch the systems....Source code would never be available to anyone.”

Cryptography pioneer Philip Zimmerman warns that “you should never trust crypto if the source code isn’t published. Open source code means two things: if there are deliberate backdoors in the crypto, peer review will reveal those backdoors. If there are inadvertent bugs in the crypto, they too will be discovered. Whether the weaknesses are by accident or design, they will be found. If the weakness is by design, they will not want to publish the source code. Some of the best products we know have been subject to open source review: Linux; Apache. The most respected crypto products have been tested through open source. The little padlock in the corner when you visit a browser? You’re going through a protocol called Secure Socket Layer. Open source tested and an Internet standard. FireFox, the popular and highly secure browser, is all open source.”

THE CALEA CONNECTION

None of U.S. law enforcement’s problems with Amdocs and Verint could have come to pass without the changes mandated by the Communications Assistance for Law Enforcement Act of 1994, which, as noted, sought to lock spyware into telecom networks. CALEA, to cite the literature, requires that terrestrial carriers, cellular phone services and other telecom entities enable the government to intercept “all wire and oral communications carried by the carrier concurrently with their transmission.” T2S2 technology fit the bill perfectly: Tied into the network, T2S2 bifurcates the line without interrupting the data-stream (a T2S2 bifurcation is considered virtually undetectable). One half of the bifurcated line is recorded and stored in a remote tapping room; the other half continues on its way from your mouth or keyboard to your friend's. (What is "T2S2"? To simplify: The S2 computer collects and encrypts the data; the T2 receives and decrypts.)

CALEA was touted as a law enforcement triumph, the work of decades of lobbying by FBI. Director Louis Freeh went so far as to call it the bureau's "highest legislative priority." Indeed, CALEA was the widest expansion of the government's electronic surveillance powers since the Crime Control and Safe Streets Act of 1968, which mandated carefully limited conditions for wiretaps. Now the government could use coercive powers in ordering telecom providers to "devise solutions" to law enforcement's "emerging technology-generated problems" (imposing a $10,000 per day penalty on non-compliant carriers). The government's hand would be permanently inserted into the design of the nation's telecom infrastructure. Law professor Lillian BeVier, of the University of Virginia, writes extensively of the problems inherent to CALEA. "The rosy scenario imagined by the drafters cannot survive a moment's reflection," BeVier observes. "While it is conventionally portrayed as 'but the latest chapter in the thirty year history of the federal wiretap laws,' CALEA is not simply the next installment of a technologically impelled statutory evolution. Instead, in terms of the nature and magnitude of the interests it purports to 'compromise' and the industry it seeks to regulate, in terms of the extent to which it purports to coerce private sector solutions to public sector problems, and in terms of the foothold it gives government to control the design of telecommunications networks, the Act is a paradigm shift. On close and disinterested inspection, moreover, CALEA appears to embody potentially wrong-headed sacrifices of privacy principles, flawed and incomplete conceptions of law enforcement's ends and means, and an imperfect appreciation of the incompatible incentives of the players in the game that would inevitably be played in the process of its implementation."(emphasis mine)

The real novelty – and the danger – of CALEA is that telecom networks are today configured so that they are vulnerable to surveillance. "We've deliberately weakened the computer and phone networks, making them much less secure, much more vulnerable both to legal surveillance and illegal hacking," says former DOJ cybercrimes prosecutor Mark Rasch. "Everybody is much less secure in their communications since the adopting of CALEA. So how are you going to have secure communications? You have to secure the communications themselves, because you cannot have a secure network. To do this, you need encryption. What CALEA forced businesses and individuals to do is go to third parties to purchase encryption technology. What is the major country that the U.S. purchases IT encryption from overseas? I would say it's a small Middle Eastern democracy. What we've done is the worst of all worlds. We've made sure that most communications are subject to hacking and interception by bad guys. At the same time, the bad guys – organized crime, terrorist operations – can very easily encrypt their communications." It is notable that the first CALEA-compliant telecom systems installed in the U.S. were courtesy of Verint Inc.

THE AMDOCS CONNECTION

If a phone is dialed in the U.S., Amdocs Ltd. likely has a record of it, which includes who you dialed and how long you spoke. This is known as transactional call data. Amdocs' biggest customers in the U.S. are AT&T and Verizon, which have collaborated widely with the Bush

Administration’s warrantless wiretapping programs.   Transactional call data has been identified as a key element in NSA data mining to look for “suspicious” patterns in communications.

Over the last decade, Amdocs has been the target of several investigations looking into whether individuals within the company shared sensitive U.S. government data with organized crime elements and Israeli intelligence services. Beginning in 1997, the FBI conducted a far-flung inquiry into alleged spying by an Israeli employee of Amdocs, who worked on a telephone billing program purchased by the CIA. According to Paul Rodriguez and J. Michael Waller, of Insight Magazine, which broke the story in May of 2000, the targeted Israeli had apparently also facilitated the tapping of telephone lines at the Clinton White House (recall Monica Lewinsky’s testimony before Ken Starr: the president, she claimed, had warned her that “a foreign embassy” was listening to their phone sex, though Clinton under oath later denied saying this). More than two dozen intelligence, counterintelligence, law-enforcement and other officials told Insight that a “daring operation,” run by Israeli intelligence, had “intercepted telephone and modem communications on some of the most sensitive lines of the U.S. government on an ongoing basis.” Insight’s chief investigative reporter, Paul Rodriguez, told me in an e-mail that the May 2000 spy probe story “was (and is) one of the strangest I've ever worked on, considering the state of alert, concern and puzzlement” among federal agents.   According to the Insight report, FBI investigators were particularly unnerved over discovering the targeted Israeli subcontractor had somehow gotten his hands on the FBI’s “most sensitive telephone numbers, including the Bureau's ‘black’ lines used for wiretapping.” “Some of the listed numbers,” the Insight article added, “were lines that FBI counterintelligence used to keep track of the suspected Israeli spy operation. The hunted were tracking the hunters.” Rodriguez confirmed the panic this caused in American intel. “It's a huge security nightmare,” one senior U.S. official told him. “The implications are severe,” said a second official. “All I can tell you is that we think we know how it was done,” a third intelligence executive told Rodriguez. “That alone is serious enough, but it's the unknown that has such deep consequences.” No charges, however, were made public in the case. (What happened behind the scenes depends on who you talk to in law enforcement: When FBI counterintelligence sought a warrant for the Israeli subcontractor, the Justice Department strangely refused to cooperate, and in the end no warrant was issued. FBI investigators were baffled.)

London Sunday Times reporter Uzi Mahnaimi quotes sources in Tel Aviv saying that during this period e-mails from President Clinton had also been intercepted by Israeli intelligence. Mahnaimi’s May 2000 article reveals that the operation involved “hacking into White House computer systems during intense speculation about the direction of the peace process.”   Israeli intelligence had allegedly infiltrated a company called Telrad, subcontracted by Nortel, to develop a communications system for the White House. According to the Sunday Times, “Company managers were said to have been unaware that virtually undetectable chips installed during manufacture made it possible for outside agents to tap into the flow of data from the White House.”

In 1997, detectives with the Los Angeles Police Department, working in tandem with the Secret Service, FBI, and DEA, found themselves suffering a similar inexplicable collapse in communications security. LAPD was investigating Israeli organized crime: drug runners and credit card thieves based in Israel and L.A., with tentacles in New York, Miami, Las Vegas, and

Egypt.   The name of the crime group and its members remains classified in “threat assessment” papers this reporter obtained from LAPD, but the documents list in some detail the colorful scope of the group’s operations: $1.4 million stolen from Fidelity Investments in Boston through sophisticated computer fraud; extortion and kidnapping of Israelis in L.A. and New York; cocaine distribution in connection with Italian, Russian, Armenian and Mexican organized crime; money laundering; and murder.   The group also had access to extremely sophisticated counter-surveillance technology and data, which was a disaster for LAPD.   According to LAPD internal documents, the Israeli crime group obtained the unlisted home phone, cell phone, and pager numbers of some 500 of LAPD’s narcotics investigators, as well as the contact information for scores of federal agents – black info, numbers unknown even to the investigators’ kin. The Israelis even set up wiretaps of LAPD investigators, grabbing from cell-phones and landlines conversations with other agents – FBI and DEA, mostly – whose names and phone numbers were also traced and grabbed.

LAPD was horrified, and as the word got out of the seeming total breakdown in security, the shock spread to agents at DEA, FBI and even CIA, who together spearheaded an investigation. It turned out that the source of much of this black intel could be traced to a company called J&J Beepers, which was getting its phone numbers from a billing service that happened to be a subsidiary of Amdocs.

A source familiar with the inquiries into Amdocs put to me several theories regarding the allegations of espionage against the company. “Back in the early 1970s, when it became clear that AT&T was going to be broken up and that there was an imminent information and technology revolution, Israel understood that it had a highly-educated and highly-worldly population and it made a few calculated economic and diplomatic discoveries,” the source says. “One was that telecommunications was something they could do: because it doesn’t require natural resources, but just intellect, training and cash. They became highly involved in telecommunications. Per capita, Israel is probably the strongest telecommunications nation in the world. AT&T break-up occurs in 1984; Internet technology explodes; and Israel has all of these companies aggressively buying up contracts in the form of companies like Amdocs. Amdocs started out as a tiny company and now it’s the biggest billing service for telecommunications in the world. They get this massive telecommunications network underway.   Like just about everything in Israel, it’s a government sponsored undertaking.

“So it’s been argued that Amdocs was using its billing records as an intelligence-gathering exercise because its executive board over the years has been heavily peopled by retired and current members of the Israeli government and military. They used this as an opportunity to collect information about worldwide telephone calls. As an intelligence-gathering phenomenon, an analyst with an MIT degree in algorithms would rather have 50 pages of who called who than 50 hours of actual conversation. Think about conversations with friends, husbands, wives. That raw information doesn’t mean anything. But if there’s a pattern of 30 phone calls over the course of a day, that can mean a lot. It’s a much simpler algorithm.”

Another anonymous source – a former CIA operative – tells me that U.S. intelligence agents who have aired their concerns about Verint and Amdocs have found themselves attacked from all sides. “Once it’s learned that an individual is doing footwork on this [the Verint/Amdocs question], he or she is typically identified somehow as a troublemaker, an instigator, and is hammered mercilessly," says the former CIA operative. "Typically, what happens is the individual finds him or herself in a scenario where their retirement is jeopardized – and worse. The fact that if you simply take a look at this question, all of a sudden you're an Arabist or anti-Semitic – it's pure baloney, because I will tell you first-hand that people whose heritage lies back in that country have heavily worked this matter.   You can't buy that kind of dedication."

The former CIA operative adds, "There is no defined policy, at this time, for how to deal with this [security issues involving Israel] – other than wall it off, contain it. It's not cutting it. Not after 9/11. The funeral pyre that burned on for months at the bottom of the rubble told a lot of people they did not need to be 'politically correct.' The communications nexuses [i.e. Amdocs/Verint] didn't occur yesterday; they started many years ago. And that's a major embarrassment to organizations that would like to say they're on top of things and not co-opted or compromised. As you start to work this, you soon learn that many people have either looked the other way or have been co-opted along the way. Some people, when they figure out what has occurred, are highly embarrassed to realize that they've been duped. Because many of them are bureaucrats, they don't want to be made to look as stupid as they are. So they just go along with it. Sometimes, it's just that simple."

Source...