Verizon Communications

Canada Pension Plan Investments

2012 shares = $159 million
(Direct & indirect investments)

2011 shares = $55 million
(Direct investments only)

Bridging the gap between communications and mass surveillance.

Although technically a global broadband/telecom company, Verizon provides the mass surveillance and data-analysis services of a gargantuan privatized intelligence agency. Originally founded in 1984, as Bell Atlantic Corp., it was one of seven "Baby Bells" created when antitrust legislation forced the breakup of the illegal monopoly controlled by "Ma Bell," aka, the American Telephone & Telegraph Co. (AT&T).

Since then, Verizon has acquired assets of US$220 billion. Its success has come, in part, from working closely with military and intelligence agencies in a variety of countries, especially the US. Calling itself "the largest provider of communications services to the US federal government," Verizon also says it has been "serving the intelligence community for more than 25 years."

US government data for 2000 to 2009 shows that of the US$5.2 billion in Verizon contracts with the US federal government, about US$4 billion were with military, law enforcement and intelligence entities, including the Army, Navy, Air Force and FBI. About half of Verizon's government contracts (US$2.48 billion) were with the "Defense Information Systems Agency." This "Combat Support Agency" describes its mission by saying: "We facilitate use of real time intelligence, surveillance, and reconnaissance information to enable information exchange between the producer and the shooter," and "We must enable information dominance as we support the new global warfighter on-the-move."

While Verizon provides what it slyly calls "Bullet Proof Network Operations and Security Centres" to shield government secrets, it has not protected citizens' privacy. Like AT&T, Verizon was caught in a major scandal. Whistleblower Thomas Tamm., a Justice Department lawyer with the Office of Intelligence Policy and Review, revealed that AT&T intercepted billions of messages per day and violated the Foreign Intelligence Surveillance Act. This law governs national security investigations, controls wiretapping and surveillance technologies, and requires compliance with constitutional injunctions against warrantless search and seizure.

When confronted by the House of Representatives, Verizon admitted giving customers' internet communications and phone call data to the National Security Agency (NSA) between 2005 and 2007. This was done, Verizon said, 720 times when the NSA did not have warrants, and 94,000 times when such legal documents were provided.

In 2008, another whistleblower, Babak Pasdar, said his unnamed telecom client gave the FBI total access to all their customers' voice communications and electronic data. The *Washington Post* revealed the firm in question was Verizon. Pasdar said Verizon

> "listened in and recorded all conversations en-masse; collected and recorded mobile phone data use en-masse; obtained data that the company accessed from mobile phone usage, including internet access, e-mail and web browsing; trended calling patterns and call behavior; identified inbound and outbound callers; tracked all inbound and outbound calls; and traced a user's physical location."

Later that year, the US Congress passed a law granting blanket immunity to telecom companies and the Bush administration from prosecution for all of this illegal electronic surveillance.

The Israeli connection to this huge scandal is found in Israeli companies used to facilitate this mass warrantless surveillance. ATT used technology and software from Israel's Narus, while Verizon chose another Israeli spy company called Verint Systems. (See previous issue, pp.48-49.)

Verint is a subsidiary of Comverse Technology, "the world's leading provider of…communications intercept and analysis" technology. Founded in Israel and with half its employees based there, Comverse and many of its key executives have long been intimately linked to Israel's military and intelligence agencies.

Verint's cofounder and chair (from 1994 until 2006) was "Kobi" Alexander who had worked for Israel's military intelligence. In 2006, he fled the US to Israel and then Namibia to evade 36 charges of conspiracy, fraud and money laundering while at Verint.

In describing Verint's role in providing mass surveillance technologies to Verizon, investigative journalist James Bamford noted 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 [Verint] run by former Israeli military and intelligence officers."

This problem with Verint spyware was not limited to US users like Verizon. In 2003, a Dutch technology magazine, *c't*, revealed that all of the

"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 in question was T2S2 tapware "delivered to the [Dutch] government in the last few years by the Israeli company Verint."

In 2004, Australian MPs complained about Verint spy technology that was being used by "at least six different law enforcement agencies" in Australia. Their concerns included Verint ability to access Australian data from Israel. Bamford called it "unnerving" "that Verint can...access the megaterabytes of stored and real-time data secretly and remotely from anywhere, including Israel."

Verizon should have known better than to let Verint access billions of private, daily messages. By turning over all this sensitive data to the Israeli spy company, Verizon is complicit in a security breach of gargantuan proportions. As Bamford concludes that the:

"greatest potential beneficiaries of this marriage between the Israeli eavesdroppers and America's increasingly centralized telecom grid, are Israel's intelligence agencies."

References

Verizon 2010 10-K Annual Report
www.sec.gov/Archives/edgar/data/732712/000119312511049476/dex13.htm

Verizon, Wikipedia
en.wikipedia.org/wiki/Verizon

National Intelligence Sector
www.verizonbusiness.com/worldwide/solutions/government/federal/nis/

Contracts to Verizon Communications
www.fedspending.org/fpds/search.php

Martin H. Bosworth, "Verizon Gave Customer Data To Government Without Court Orders," *Consumer Affairs*, October 16, 2007.
www.consumeraffairs.com/news04/2007/10/verizon_surveillance.html

Tom Burghardt, "Thick as Thieves: The Private (and very profitable) World of Corporate Spying," *Pacific Free Press*, November 30, 2008.
www.pacificfreepress.com/news/1-/3385-the-private-and-profitable-world-o

James Bamford, "The Shadow Factory, the Ultra-Secret NSA from 9/11 to the Eavesdropping on America," 2008.

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

Bridging the gap between "Cloud Computing" and the reality of war

VMWare Inc.

Canada Pension Plan Investments

2012 shares = $20 million
(Direct & indirect investments)

2011 shares = $7 million
(Direct investments only)

VMWare is a US-based information technology company which calls itself "the global leader in virtual infrastructure software." Its "cloud computing" products are designed to increase the efficiency of computer resources and reduce costs through "virtualization."

Although the VM in VMWare stands for Virtual Machine, the physical reality of wars fought with the benefit of VMWare products is anything but artificial. Among VMWare's most prized customers, it says, are the "world's largest companies," as well as various military and spy agencies. In fact, when VMWare lists its US government clients, it puts the "Department of Defense" at the very top. VMWare also proudly includes the US "Intelligence Community" on this customer list. VMWare also promotes itself by saying that it services America's top 15 aerospace and "defense" companies.

VMWare is a subsidiary of EMC Corp. which acquired it for US$625 million in 2003. EMC is a US-based IT company serving various armed forces including the Israeli military. (See previous issue, p.30.)

VMWare's virtualization products have long been used by the Israel Defense Forces (IDF). In 2009, Israel's *Globes* business paper reported that the IDF had just awarded its "first virtualization tender" – a US$15 million contract to install VMWare software on IDF computers. This three-year contract, with a two-year option to extend, was won by Hewlett Packard. (See previous issue, pp.36-37.)

This, *Globes* also revealed, was not the first time that the IDF installed VMWare software on its computers. In 2008, an IDF spokesperson was quoted in *Globes* saying that VMware "software was purchased from IBM as part of a procurement of servers." That purchase, it said, was part of a three-year US$60-million contract with IBM which "included virtualization servers of VMware." Israel's military spokesperson also said "[t]he IDF has used VMware software for a long time."

References

VMware Customers
www.vmware.com/il/company/customers

EMC Completes Acquisition of VMware
www.vmware.com/company/news/releases/emc2.html

Support Mission-Critical Government Initiatives with VMware
www.vmware.com/industry/government/index.html

Shmulik Shelah, "HP beats IBM in Army virtualization tender," *Globes*, July 15, 2009
www.globes.co.il/serveen/globes/docview.asp?did=1000481161

"IDF spends $6-7m on VMware virtual servers," *Globes*, February 21, 2008.
www.globes.co.il/serveen/globes/docview.asp?did=1000312774

Shmulik Shelah, "IDF publishes $15m virtualization tender," *Globes*, May 4, 2009.
www.globes.co.il/serveen/globes/docview.asp?did=1000446612