Verisign Inc.

Canada Pension Plan Investments

2012 shares = $56 million
(Direct & indirect investments)

2011 shares = $66 million
(Direct investments only)

This US-based company, which is coincidentally a mere 20-minute drive from CIA headquarters, has very close ties to the intelligence community. Verisign is also very well-located on the global information highway. According to information-technology journalist, Kieren McCarthy, Verisign "originally possessed almost complete control of the internet."

Verisign still controls some of the web's biggest root nameservers, including all internet sites ending with the .com, .net, .org and .edu suffixes. And, Verisign is happy to share its inside knowledge about how people use the web, with entities like the US Department of "Homeland Security."

Verisign's control over .com and .net domains alone have given it 93 million of the world's 184 million registered websites. Until late 2010, when it sold its electronic authentication unit to Symantec, Verisign was the world's largest provider of digital certificates.

In 1995, Verisign spun off from RSA Security, a division of EMC Corp. (See previous issue, p.30.) Its assets have grown to US$2.4 billion, and annual revenues are at US$680 million.

Because of its powerful roles in the business of running the internet's infrastructure, Verisign is in a position to observe exactly what millions of people are doing online. Stratton Sclavos, who cofounded Verisign and has been its president, CEO and chairman, is now a Senior Advisor to the US Director of National Intelligence who councils the US President, the National Security Council and the Homeland Security Council on intelligence issues. In a 2005 interview, Sclavos revealed that Verisign has "shared our technology and our software-monitoring tools with the Department of Homeland Security [DHS] since almost its first days" and had "just agreed to the same kind of provisions with the European Union."

www.verisigninc.com/assets/datasheet-idefense-solutions-overview.pdf

VERISIGN® iDEFENSE® SECURITY INTELLIGENCE SERVICES

When asked about Verisign's links to the DHS, and whether the company is "involved with the war on terrorism," Sclavos replied:

> "We are an avid participant in their information-sharing private-public partnership. We provide them tools that we have designed so that they can see the network and its trouble the same way we can, and then we're involved in certain forensic activities on an as-needed basis."

A current Verisign board member, Kenneth Silva, joined the firm in 2000, and served as chief security officer, chief technology officer and senior vice president. Before that, Silva worked for the US National Security Agency (NSA) and was its executive technical director for nine years. For 11 years before that, he was a senior analyst with the US Air Force.

Besides assisting the DHS, Verisign helps large internet companies comply with requests from police and spy agencies. To conduct this privatized intelligence work, Verisign partnered with two Israeli spy firms that played central roles in the Bush-era warrantless-wiretapping scandal. Both companies, Narus and Verint Systems, have ties to the Israeli military and intelligence communities. (See previous issue, pp.43-47.) The mass-surveillance spying tools created by Narus and Verint were used to gather vast amounts of private internet data for the NSA, by AT&T and Verizon, respectively. (See "ATT," in the previous issue, p.7, and "Verizon" in this issue, p.48-49.)

Verisign also has its own internet surveillance product called NetDiscovery which has absorbed the spying technologies of both Verint and Narus. In 2002, Verisign announced that Verint's "STAR-GATE communications interception product" would

> "provide VeriSign with the technology to intercept communications across various switching systems and the means to deliver intercepted communications content and call data to law enforcement agencies."

Then in 2005, Narus said that it had "signed an agreement with Verisign" to provide it with an internet "monitoring system that can be implemented at the network core to analyze and correlate traffic in real-time" to collect "subscriber information, historical billing, [and] call detail records."

Verisign, and its Israeli-linked partners Verint and Narus, have been instrumental in creating what telecom industry writer Annalee Newitz aptly dubbed "the Wiretap Friendly Web."

Since 2003, Verisign has been exclusively represented in Israel by Comsign. Comsign was appointed by Israel's Justice Ministry to be "the only entity issuing legal authorized electronic signatures" in Israel. As "VeriSign's certificate authority in Israel," Comsign has the monopoly on Israel's "digital authentication certificates."

This is significant because, as a representative of Comsign's parent company, Comda Ltd, explains, "[e]ntire segments of the [Israeli] public" and the "the Defense Ministry" are required to have an "electronic signature." Comsign also issues electronic signatures to "judges and court administration staff…[and] security officers."

Comsign's customers in Israel include Pelephone (wholly-owned by Bezeq), as well as Cellcom, Leumi

Verisign hypes the "War on Terror" with fear-mongering about "Muslim hackers," "Islamic Hacktivism," "militant Islamist movements" and "militant jihadists" allied with "cyber criminals," "Islamic cyber cartels" and "Muslim extremists" who "use cyber fraud" to fund terrorism.

Le'Israel and Partner Communications. (See previous issue, pp.11, 17, and this issue, pp.13-14 and 29.) Another corporate client, named "#6 Road operator," manages Israel's Highway #6. This major toll road, also known as the Itzhak Rabin Highway, is described in *Apartheid Roads: Promoting Settlements, Punishing Palestinians*, as one of the "Main Israeli-only Roads" which help to "provide a fast link for the colonies to most locations inside Israel."

Through the creation of a business called iDefense, Verisign also serves as a private intelligence agency providing "Security Intelligence Services" to "information security executives." iDefense says it offers "24/7 access to accurate and actionable cyber intelligence related to vulnerabilities, malicious code, and global threats."

However, Rob Rosenberger, the co-founder/editor of Vmyths, a website reporting the "Truth About Computer Security Hysteria," has a very different view of iDefense. In a scathing critique, Rosenberger describes its 2001 "Israeli-Palestinian Cyber Conflict" report as "fearmongering." He notes that it "uses the right trigger words," pie charts, graphics, and even "genuine hate language in an obvious attempt to make the cyber-war seem dire." iDefense, Rosenberger says, "wants you to think they monitor 'escalating cyber attacks' in the Gaza region." However, "[i]n reality," he says, Verisign's reports merely document

> "a bunch of teenage hacker wannabees who lob ping packets at each other. iDefense knows reporters have a fetish for juicy computer security stories, so they prostitute themselves in return for publicity."

Since 2001, Verisign's Middle-East reports have gone from bad to far worse. In the iDefense Security Intelligence Team's "2009 Cyber Threats and Trends" report, there is a section on "The Greater Middle East and Central Asia." The report contains no mention of any threats posed by pro-Israeli individuals or organisations, let alone the Israeli military, police or intelligence forces. Instead, iDefense focuses entirely on what it calls "militant Islamic use of online resources." Smacking of Islamophobia, this Verisign report refers to "Muslim hackers," "Islamic Hacktivism," cyber-threats from "indigenous militant Islamist movements," and "militant jihadists" that collaborate with "cyber criminals." Verisign's iDefense report also hypes up the threat of "cyber fraud operations in support of Islam," and speaks of "Islamic cyber cartels" and "Muslim extremists …[who] justify the use [of] cyber fraud …to fund their agendas." iDefense also gives extremely dire warnings about

> "the propensity among Middle Eastern hackers — particularly Arabic-speaking users with ideological leanings — to justify their actions online with religious fatwas, or Islamic decrees, no matter how tenuous their reasoning may be."

Such blatantly one-sided reports from iDefense's "Security Intelligence Teams" are no doubt lapped up 24/7 by Verisign clients in government and big business, as well as those in intelligence and law enforcement communities. These iDefense customers can then use Verisign's "intelligence" to rationalize their own biased policies and actions which ignore, or even support, Israel's military actions, its occupation of Palestinian land or its many transgressions of international law.

References

Verisign Reports 10% Year-Over-Year Revenue Growth in 2010, January 27, 2011.
https://investor.verisign.com/releasedetail.cfm?ReleaseID=546077

"VERISIGN On the Record: Stratton Sclavos," *San Francisco Chronicle*, January 9, 2005.
www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/01/09/BUG22AFFKP47.DTL#ixzz1du8nnxNw

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

Robert Poe, "The Ultimate Net Monitoring Tool," *Wired*, May 17, 2006.
www.wired.com/science/discoveries/news/2006/05/70914

"Narus Signs Agreement with VeriSign to Allow IP Compliance and Security Products to be Offered as Managed Services," Dec. 6, 2005.
www.narus.com/index.php/news/296-narus-signs-agreement-with-verisign-to-allow-ip-compliance-and-security-products-to-be-offered-as-managed-services

Verint Receives First STAR-GATE Order From VeriSign, June 3, 2002.
verint.com/corporate/releases_view.cfm?article_level1_category_id=7&article_level1_id=263&pageno=2&year=2002

Mark G. Levey, "NSA Scandal: NeuStar - Telcom Scapegoat or NSA Front Company?" *Daily KOS*, May 20, 2006.
www.dailykos.com/story/2006/05/20/212011/-NSA-SCANDAL:-NeuStarTelcom-Scapegoat-or-NSA-Front-Company

Mark G. Levey, "NSA Scandal (Pt. 2): Verint – NSA's Foreign Partner," *Democratic Underground*, May 26, 2006.
www.democraticunderground.com/discuss/duboard.php?az=view_all&address=364x1290021

Annalee Newitz, "Milking the Internet surveillance cash cow: Wiretap-friendly Web," *Enterprise Security*, April 6, 2004.
www.theregister.co.uk/2004/04/06/fbi_wiretap_bonanza/page2.html

Kenneth J. Silva
investing.businessweek.com/businessweek/research/stocks/people/person.asp?personId=22102292

Stratton D. Sclavos
investing.businessweek.com/research/stocks/private/person.asp?personId=223389

About us
www.comda.co.il/eng/main.asp?id=31

Hila Yaakobi, "Comda - Envisioning a Transition to a Secure, Efficient and Paper-Free Electronic World," Jobnet
www.jobnet.co.il/content.aspx?Category=961

Profile
www.comsign.co.il/eng/main.asp?id=103

ComsignTrust, June 2009.
www.comsigntrust.com/userfiles//ComSignTrust%20%20authomated%20system%20for%20electronic%20signatures.pdf

iDefense Security Intelligence Services
www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/index.xhtml

Rob Rosenberger, "Raid on E-tebbe, part 5," *Vmyths*, March 13, 2001.
vmyths.com/column/1/2001/3/13/

2009 Cyber Threats and Trends, Dec. 12, 2008.
www.verisigninc.com/assets/whitepaper-idefense-2009trends.pdf