The holes in a pay TV pirate's defence

A legal judgment in its favour has done little to quell suspicions of News Corp subsidiary NDS's involvement in pay TV piracy, as more evidence comes to light.

Neil Chenoweth

It was hailed as a great victory – a vindication that would silence the critics.

Finally, after five multibillion-dollar court actions spanning 11 years, Abe Peled, the executive chairman of News Corporation's controversial technology arm, NDS Limited, was awarded $18.9 million for legal costs.

Peled could unequivocally lay to rest claims that NDS had promoted pay TV piracy.

But within days of the US court's ruling last month, Peled faced a new legal threat, from Mark Lewis, the British lawyer representing many of the UK telephone hacking victims suing News International.

Lewis has revealed he is investigating allegations against NDS by an unnamed client in the UK and the US which he said were "uncannily similar" to events reported in *The Australian Financial Review*.

His investigations are continuing against the broader telephone hacking inquiry, with the Commerce Committee of the US Senate this week asking the Leveson inquiry for evidence of possible illegal acts by News Corp subsidiaries, after the UK parliamentary committee finding that Rupert Murdoch is "not fit" to run a major company and News Corp directors were "wilfully blind" to a cover up.

The *Financial Review* has linked NDS to dirty tricks operations around the world that promoted piracy of News Corp's rivals in a series of articles based in part on an archive of more than 14,000 internal NDS emails, which are being progressively published on the *Financial Review* website.

Within days of his announcement, Lewis says, NDS lawyers contacted him to say that any such events would be beyond the statute of limitations. NDS has vigorously denied the *Financial Review*'s reports and says they are based on misinterpretations of the emails.

NDS has been sued by five of the largest satellite broadcasters in the world with separate claims totalling $5 billion that it promoted piracy of their systems – EchoStar and DirecTV (twice) in the US, Canal Plus and Sogecable in Europe and Astro in Malaysia, but EchoStar is the only case that went to trial.

The *Financial Review* reviewed the 2700 pages of transcripts from the EchoStar trial, and spoke with members of the jury in 2009 (permitted under US law) together with a string of witnesses who testified – as well as others close to the case who didn't.

The jury included an IT manager, a HR consultant, a senior hospital executive, a biology researcher and retailers.

NDS did not respond to questions about the case.

The picture that emerges is a lawsuit that was crippled by the statute of limitations, rendering much potential evidence inadmissible. "It completely killed us – our strongest evidence was based on an earlier period," says Alan Guggenheim, the French-born executive who oversaw piracy investigations for EchoStar and for Kudelski Corporation. Kudelski is the Swiss company that provided the technology to protect EchoStar from piracy through a joint-venture company with EchoStar called NagraStar.

The long road to the EchoStar court case, as Guggenheim recalls it, began with a meeting at the Los Angeles offices of EchoStar's rival, DirecTV, on November 3, 1998.

Pay television companies use encryption security to ensure that only paid-up customers can watch their programs, using a smartcard that unlocks the programming.

But when hackers manage to crack these smartcards, they can sell pirate cards which unlock the programming for free – with devastating effects on the pay TV company's earnings.

DirecTV used NDS smartcards, which had been widely pirated, and wanted to switch to Kudelski's piracy-free Nagra cards.

Guggenheim told the *Financial Review* in an interview in his home in Texas that the DirecTV contract was worth $90 million a year. He said based on feedback from DirecTV: "In my mind we had already won it."

Then the bombshell hit. During a coffee break, DirecTV's director of technical engineering, Ray Kahn, quietly told the Kudelski team that their EchoStar Nagra card might have been attacked and gave technical details related to the attack. Guggenheim was stunned by Kahn's revelations. Kahn was right – some of the Nagra card's source code had been published on a Canadian website called DR7 11 days before by someone calling themselves Swiss Cheese Productions.

Almost 10 years later the 2008 trial would throw up an unusual coincidence. NDS had a "Black Hat" team of hackers based in Haifa, Israel, trained by German master hacker Oliver Kömmerling. In 1998 they had reverse engineered (deconstructed) the smart cards of all of NDS's competitors – Nagra, Canal Plus, Irdeto and Viaccess.

They had finished a manual describing how to pirate the EchoStar card just two days before DirecTV told Guggenheim that his card had been attacked.

Was NDS behind the DirecTV claim and the Swiss Cheese posting? It's certainly possible that someone else had used a Focused Ion Beam, or even just a laser, on the Nagra card and spent six months developing a hack, at the same time as NDS did.

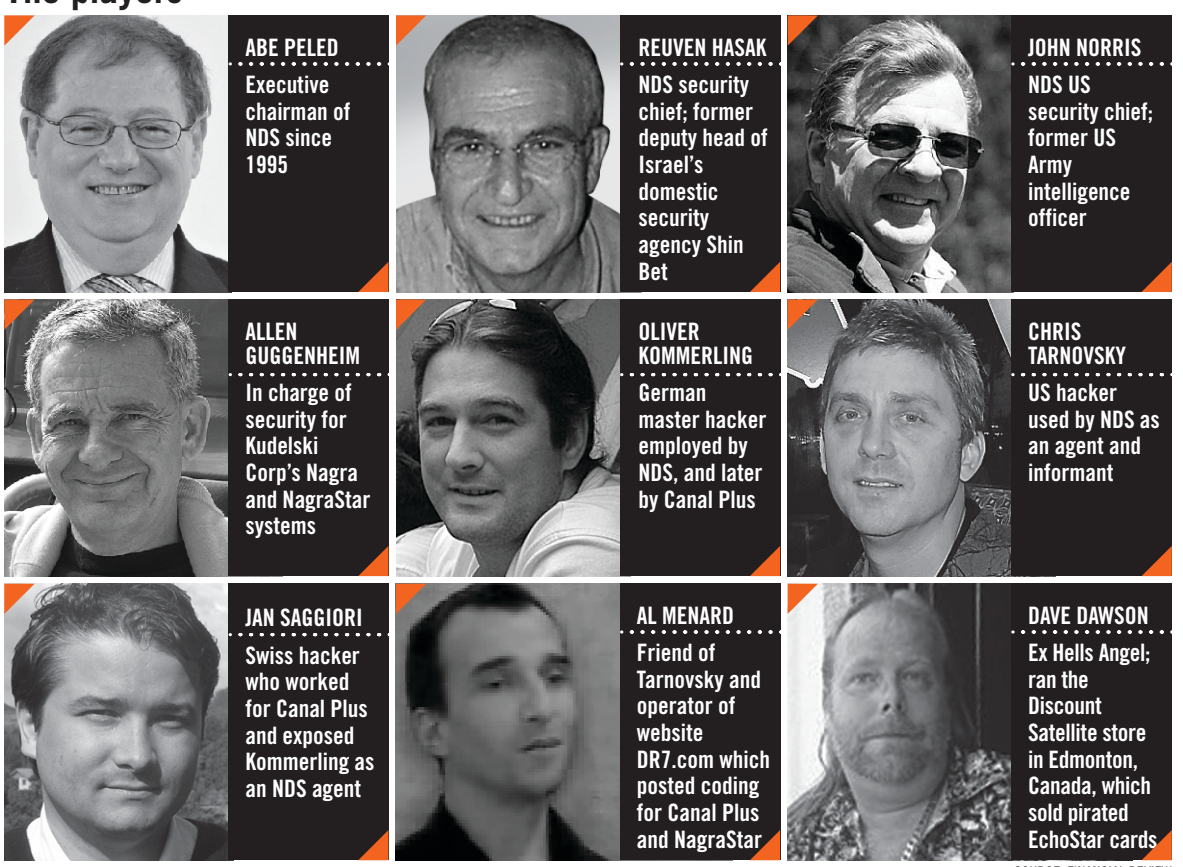
Persistent but unconfirmed reports suggested Swiss Cheese Productions was a US hacker known as "biggun" – in reality Chris Tarnovsky, an NDS employee.

Tarnovsky was a close friend of Al Menard, who ran the DR7 piracy website in Edmonton. "Al's a good guy," Tarnovsky told the *Financial Review* in an interview in southern California in 2009. "I've known him for 10, 12 years now, I mean just a normal guy, a normal Joe Blow."

The Nagra piracy killed off any prospect that Nagra would replace NDS at DirecTV – which was worth $1 billion to NDS in the next decade.

Five months later, the source code for the smartcard of another NDS rival, Canal Plus, appeared on the same DR7 website on which the EchoStar code had appeared.

The players



SOURCE: FINANCIAL REVIEW

The picture that emerges is a lawsuit crippled by the statute of limitations, rendering much evidence inadmissible.

In interviews with the BBC *Panorama* program and emails with the *Financial Review*, Oliver Kömmerling said that when he downloaded the Canal Plus file on DR7, it showed up on his computer directory as having been created at exactly the same time as the identical Canal Plus file that the NDS Black Hat team created in Haifa nine months before – July 6, 1998, at 15 seconds past 4pm.

There are 23 million seconds in a year. Two identical files, the only ones not held by Canal Plus. What are the odds that they would be created at exactly the same moment?

"This is impossible, that two people on this planet can read out the same file at the same second – I mean!," Kömmerling said.

NDS points out that it is possible to alter a time stamp on a file. But if someone was trying to "frame" NDS in March 1999, they would first need to know what the Haifa time stamp was – and only NDS knew that.

"The second part of the story I got from Tarnovsky himself," Kömmerling said. "Tarnovsky told me that he was given the code by NDS and . . . he didn't really know what to do with it."

Tarnovsky was at a dinner with Reuven Hasak, the head of NDS's Operational Security Unit, and US OpSec chief John Norris when he asked if he should put the Canal Plus file on the internet, Kömmerling says. "Tarnovsky was saying, 'Should I do this? Should I do this? Or what do you want me to do with it? Chris told me . . . it was not an order, I mean it was a, a gesture, like, 'I don't care' gesture . . . he said to me it was a kind of nodding or something like that, or whatever they called it, like a facial gesture . . . what he interpreted as 'OK, I'm doing this'."

In the 2009 interview, Tarnovsky denied putting any code on the internet. However, he told the *Financial Review* that he had "played around" with the EchoStar Nagra code – in fact, he had made it work better. "Sometimes I see through the algorithms, like, and stuff. Like the cypher in the Nagra chip. They had some shift going on at the beginning and the end. And I totally realised, well, wait a second, I can go the reverse, I can skip it, remove it, and just shift the other way. And I totally removed like – I don't know how many clock cycles of their code. And their algorithm was like – 20, 15 times faster."

A Swiss hacker, Jan Saggiori, later testified that two days after the Canal Plus file appeared on the DR7 website in March 1999, Tarnovsky sent him a file with part of the system code for the smartcard used by EchoStar.

It's a crucial piece of evidence for technical reasons. The file was encrypted with PGP, a system that authenticates both the time that it was sent and the contents.

The NDS expert at the 2008 trial did not contest the legitimacy of the PGP file. Tarnovsky said the email must have been fabricated.

Back in 1999, Guggenheim says DirecTV execs and several law enforcement officers suggested NDS was responsible for a wave of EchoStar piracy. "I was not believing it for a very long time," Guggenheim told the *Financial Review*. "I was the sceptic and thinking, 'OK you have to prove it to me, because I think they have too much to lose to do something like that.'"

Yet another anomaly aroused Guggenheim's suspicions. Pirates who hack a pay TV system invariably sell the original hack over and over again to pirate dealers to maximise returns. But in this case, Guggenheim's investigators found that only three Canadian dealers were reprogramming the original EchoStar cards to make them pirate cards. Other pirate dealers could not obtain the hack.

His investigators befriended an employee at the largest of the dealers, Dave Dawson's Discount Satellite store in Edmonton, and discovered that all three dealers sent the cards to be reprogrammed at Al Menard's home.

Guggenheim believed he was on the verge of cracking the case. On March 29, Guggenheim's investigators were poised to track a shipment of cards as one of Dawson's staff carried it to Menard, before seeking search warrants.