PAY TV PIRACY

Where the emails came from

PAY TV PIRACY

Neil Chenoweth

```
   From: Gutman, Avigail
     To: Adams, Ray
   Date: 12/14/1999 5:58:42 PM
Subject: RE: damn and blast!
-------------------------------
Ray - ok, thanks.

Rest assured we are NOT doing any joint action with Irdet
would clash with our business interests (we are currently
a simulcrypt solution for the satellite and the digital-c
and other broadcasters might show interest, too. Mindport
aware of this yet, as far as I know.)

We know that Curle wanted to take action against bond (hi
were voiced both to me and to peter smart at Foxtel) but
checking with lawyers - I think the legal case is very ve
Despite his big-mouth, Bond is mindful of his rights.

(Curle certainly must know by now that he cannot use any
emails in a court. It would be counter-productive for hin
```

The 14,400 emails from which this story has emerged come from a hard drive in a laptop operated by Ray Adams, a former Metropolitan Police commander who was European chief for NDS Operational Security from January 1996 to May 2002.

The emails, which come from several different folders within that drive – thus there is some duplication – were passed to *The Australian Financial Review* by an anonymous source. The *Financial Review* has undertaken its own inquiries to verify the emails.

Separate to this, the emails' authenticity is supported by:

1. The internal consistency and verifiability of many details within the vast body of documents.

2. While the emails have been converted to text files, they include the internet headers, which contain unique information about the email and the path taken in its delivery.

3. About 2000 of the emails are in PGP encrypted form. These messages have been encrypted with the public PGP keys of the recipients, many of them NDS employees. The text files include the public PGP keys of many of these recipients. These public keys can be used to verify that the messages were indeed encrypted to the email recipients. The recipients are still able to open the messages today, with their private PGP keys, which also provide the date and time when the message was sent.

When Ray Adams stepped down as European head of NDS Operational Security in May 2002, his successor, former chief inspector Len Withall, went to Adams' home in Windsor in the UK to retrieve his laptop, his mobile phone and his laptop. The head of Operational Security, Reuven Hasak, testified in a 2008 court case brought against NDS by US satellite broadcaster EchoStar that when an NDS hacker, Andy Coulthurst, examined the laptop he believed the disk had either been erased or corrupted.

One of the thousands of emails that emerged from a hard drive in a laptop operated by Ray Adams.

Withall then called Adams, who said he had replaced the hard drive. "Ray said, 'I wanted to keep the hard drive because I had some family pictures there, so come by and I'll give you the original hard drive,'" Hasak testified.

When Withall went to Adams' house the following day, Adams told him someone had broken into his wife's car and stolen several items including the hard drive, which was on the front seat. Adams had reported the burglary to the police.

Hasak testified that he believed Adams had given the hard drive to someone, but did not consider that Adams was a whistleblower.

"The only thing I said was that after we are over with this trial, I am going to sue him, yes," Hasak testified.

However, NDS has taken no action against Adams.

EchoStar's lawyers later obtained a copy of the hard drive files, but were severely restricted in using them for the 2008 trial after NDS launched an unsuccessful counter-claim against EchoStar claiming that they received the files improperly.

NDS gained a court order against a Canadian pirate dealer, Gary Tocholke, in 2007 after he obtained some of the Adams files.

The hacker who got stung

From page 1

relationship with NDS. Cottle was encouraged by those working for NDS to hack into smartcards from a rival provider, Irdeto, but at the same time NDS was concerned Cottle might turn his attention to their own pay TV platform.

It was former Metropolitan Police commander Ray Adams, who had joined Operational Security as its European chief in 1996, who suggested spying on the Sydney engineer.

"Getting his itemised telephone billing would tell us who he is in contact with abroad. Do you have resources to do that?" Adams asked Gutman in January 2000.

Gutman, who juggled a semi-public role as the wife of the Israeli consul in Taiwan with her job at NDS, told Adams this was illegal.

"Many who have attempted 'other means' were caught (including PIs, who were 'shut down')," she wrote in an email to Adams.

"What say you . . .?"

It was illegal in Britain as well, but Adams, who ran a network of 18 agents and informants as the European chief for this secretive arm of Rupert Murdoch's empire, did it nevertheless.

Eight weeks before his email exchange with Gutman, Adams had obtained two months' of phone records belonging to a piracy suspect who lived in Canada, through what he described as "the agent". He was in the process of applying for a third month of records, according to an email he sent to the US head of Operational Security, John Norris.

Adams was in the market for surveillance gear. Days later Lee Gibling, who ran the piracy website thoic.com, which was secretly funded and controlled by Operational Security, wrote to Adams, who had recruited Gibling.

Photo: LOUIE DOUVIS

Sydney hacker David Cottle says NDS is most likely making him a scapegoat.

He said he had been offered a device to eavesdrop on mobile phone calls for £6000. Adams forwarded the email to a German consultant to NDS, asking: "Can you do better?"

In January 2000, when Adams first suggested targeting Cottle's phone records, he and Gutman wanted to find names of the hackers Cottle was calling in Europe.

No further moves were made on Cottle's telephone records until August 2000.

By now, Gutman's need to know who Cottle was talking to had become compelling.

"We know EVERYTHING about him (really every single detail...)," she told Adams. "The one thing we cannot seem to get is a print out of his phonecall billings – as this is illegal to do in OZ.

"So – phone numbers are . . ."

Cottle's phone records were needed not to monitor his hacking, but to check whether he was working with NDS competitor Irdeto, whose system it was trying to replace.

Adams was unfazed. "I will need his full name and address," he replied in a return email.

Gutman supplied Cottle's address in Sydney. "I am not so much interested in Bond [Cottle's online name] as such – but I want to make sure our guys down there aren't at risk of being told about to Irdeto."

Gutman had several Australian informants who were in contact with Cottle, whom she feared could be exposed. Subsequent emails between Gutman and Adams on this subject were encrypted.

On Monday Cottle said NDS was most likely making him a scapegoat, as he had been the moderator of thoic.com.

"I think they [NDS] wanted me involved to look after the website and then, as it turned out in the end, they can point the fingers at me," he said. Cottle moderated a closed site on Thoic called Area 51, which could be accessed only by 16 of Australia's top hackers – and, unbeknown to them, Lee Gibling, Gutman, Adams and a string of Operational Security personnel.

When shown on Monday emails detailing his role in the hacking of pay TV smartcards, Cottle maintained his only role was moderating the thoic.com website.

"It's certainly news to me and I'd like to see that proof," he said.

In an email in October 1999 Gutman wrote; "Cottle is the pirate in OZ. He is a bit technical but he is mostly the leader and co-ordinator of all hacking activity there."

After the arrest of another hacker, Rolf Deubel, in Thailand in September 1999, Gutman wrote: "Cottle is the new king."

If so, he makes for an unlikely monarch. When the *Financial Review* visited Cottle at a friend's place in the outer Sydney suburb of Kenthurst, he was dressed in cut-off track suit pants and plastic sandals.

Before this the engineer was living in a modest brick veneer home in suburban Castle Hill that he recently sold for $600,000.

"I was never making a great deal of money. Look at my house, it's from the 1960s and has never been renovated," he said.

"[If I was] involved in some mastermind that is hacking pay TV, good luck. I only wish it was the case because I guess I would be living in some 50 acres in the middle of Dural."

Cottle said he was planning a move to the United States, with his wife and son, where he would "semi-retire".

NDS

Michael Clinger
CEO of NDS 1990-92. Operational Security established in part to track down Clinger whom News accused of fraud

Abe Peled ▶
CEO of NDS since July 1995

Reuven Hasak ▶
NDS security chief, former deputy head of Israel domestic security agency Shin Bet

John Norris ▶
Security chief of NDS US, former US Army intelligence. Orchestrated numerous stings against Canadian hackers

Ray Adams ▶
Security chief NDS UK, former commander Metropolitan Police criminal intelligence. Ran a network of informers and hackers for whom he offered protection from prosecution

Yossi Tsuria ▶
Chief technology officer for NDS Israel. Tsuria was part of a radical group of Jewish Israelis in the 1980s that plotted to bomb the Dome of the Rock

Avigail Gutman
NDS Operational Security, Israel and Asia. Worked on the entrapment in Thailand of Rolf Deubel, a hacker known as MadMax

NDS RIVALS

Charlie Ergen ▶
Head of EchoStar, Dish Network

Andrew Kudelski
Head of Kudelski Corporation, which produces Nagra conditional access system, used by EchoStar in US and Express BellVu in Canada

Pierre Lescure ▶
Head of Canal Plus, provider of the Seca smartcard system

Gilles Kaehlin ▶
Canal Plus security chief, former French Intelligence

Alan Guggenheim
Head of Nagra US and NagraStar

Francois Carayol
Head of Canal Plus Technologies

Larry Rissler
Head of security for DirecTV

JJ Gee
Head of security for EchoStar