THE HIGH COURT OF NEW ZEALAND **CIV 2014-485-11344**

WELLINGTON REGISTRY

Under	The Judicature Amendment Act 1972, Part 30 of the High Court Rules, the Bill of Rights Act 1990, and the Search and Surveillance Act 2012
In the matter of	An application for judicial review
And in the matter of	A search warrant issued by Judge IM Malosi of the Manukau District Court on 30 September 2014
Between	**N A HAGER** ***Applicant***
And	**HER MAJESTY'S ATTORNEY-GENERAL** ***First Respondent***
And	**THE NEW ZEALAND POLICE** ***Second Respondent***
And	**THE MANUKAU DISTRICT COURT** ***Third Respondent***

Key Evidence Bundle

Volume 3: Unbundled exhibits

Solicitor	**Counsel**	
Thomas Bennion	Julian Miles QC	Felix Geiringer
Bennion Law	Richmond Chambers	Terrace Chambers
L1, 181 Cuba Street	L5, General Buildings	No. 1 The Terrace
PO Box 25 433	33 Shortland Street	PO Box 10 201
Wellington 6146	PO Box 1008	Wellington 6143
Tel: +64 4 473 5755	Auckland 1140	Tel: +64 4 909 7297
Fax: +64 4 381 3276	Tel: + 64 9 600 5504	Fax: +64 4 909 7298
tom@bennion.co.nz	miles@richmondchambers.co.nz	felix.geiringer@terracechambers.co.nz

Index to the Key Evidence Bundle

Volume 1: Applicant's affidavits

Volume 2: Respondents' affidavits

Volume 3: Unbundled exhibits

Tab	Exhibit	Reference	Description	Date	Page
16	NAH-4	T7/p146/§36	NZ Herald article on accusation Cameron Slater attempted to procure a breach of s 249	06.06.15	280
17	DJF-2	T8/p154/§29	Article on burglar not charge after tipping of Police	20.06.13	284
18	AJB-3	T10/p183/§82	Tails software "About" page	13.03.15	285
19	A	T16/p252/§9	Brant Whale's CV	Undated	290

Volume 4: Key Police Disclosure

Tab	Exhibit	Reference	Description	Date	Page
20	LMC-1 to 15	Affidavits of Linda Marie Cheesman	Extracts from the PD bundles	Various	Original numbering

NAH-1

the guardian

New Zealand elections: dirty tricks helped John Key win another term

Nicky Hager

This is the Exhibit marked "NAH-1" referred to in the affidavit of Nicolas Alfred Hager affirmed at Wellington on 2 April 2014 before me: C A McLachlan

A ~~solicitor~~ barrister of the High Court of New Zealand

An orchestrated attack has painted Key's political opponents as dodgy, untrustworthy or incompetent. This is not how democracy should work

Wednesday 24 September 2014 05.10 BST

New Zealand's National party resoundingly won a third term in government on Saturday, despite revelations in my recent book about a dirty tricks campaign run from the prime minister's office. The book generated nation-wide interest and two major figures in the story were forced to resign. But as the voting results showed, it's arguable that the dirty tricks had already worked, smearing and destabilising political opponents and paving the way to victory.

Prime minister John Key is hailed around the world's conservative parties for his popularity, so it is important to understand what that success is built upon. First, he has cultivated an ordinary-bloke-next-door public image. He is in reality a ruthless politician (his nickname during his finance trader career was the smiling assassin) and his party is essentially a party of big business. But from the start, he created a "rags to riches" personal story and presented himself as friendly and easy going. This image remained intact for years.

Next, his government has worked systematically to close down critical voices: academics, scientists, media and more. Leaked documents in Dirty Politics show that a key tool was using National party-aligned blogs to launch personal attacks. Hundreds of people found themselves viciously derided by the bloggers (including a delight in personal and sexual smears). The leaked documents reveal that many of these attacks were initiated and supported by the National party and John Key's staff, in particular a dirty tricks coordinator named Jason

Ede working two doors along from Key's office (Ede has since resigned).

Ede's role was designed to be deniable. He was paid directly by the National party (dodging freedom on information laws), disappeared the day my book came out and was jettisoned after the election ("I think after 11 years he's decided, look, the times come for him to leave," Key said). The blogs pretended to be independent, thus also being deniable whenever the attacks generated a public backlash.

The documents also showed concerted efforts during the last two elections to trip up, distract and discredit opposing political parties. Politicians and parties are, of course, quite capable of making their own problems. But, for instance, Key's dirty tricks man went inside the Labour party's computers and dug dirt for release on a blog. The government used its access to official information to devise repeated mini scandals for launch by the bloggers. Various news organisations saw the attack bloggers as easy sources of scoops and cooperated in these manufactured scandals.

These activities have had a damaging effect on New Zealand politics, with widespread chilling of critical voices. Key's political opponents have been painted as dodgy, untrustworthy or incompetent. It was no surprise at all that he has stayed high in the polls and won the election on Saturday.

The tell-tale signs were unusual levels of personal attacks, many instances of people being targeted for being outspoken, an unusual nastiness to the attacks, the use of arms-length allies to conduct attacks and a relentless series of targeted scandals, usually of little ultimate substance and appearing in the news out of nowhere. These things are not normal in New Zealand politics, including in the National party. Key had been attracted to the political benefits of negative campaigning without wanting to be accountable for the dirty tactics. Secrecy was an essential component.

US Republican party political strategists call this a two-track approach: seeking to benefit from attack politics without risking a public backlash for stooping to negative tactics. Track one is the political leader who apparently remains clean and positive. Track two is the apparently

independent allies who conduct attack politics on the leader's behalf.

Negative politics often results large groups of people turning off politics and falling voter turnout. This was one of the results in Saturday's election. Right-wing parties bet that the people turned off voting are are more likely to support their opponents.

There is no easy answer to these anti-democratic tactics. You cannot legislate against dirty tricks and manipulation. The best defences are greater transparency (including bringing ministerial and parliamentary activities under freedom of information laws); greatly increased resources and independence for public news organisations; removing corporate funding from parties and election campaigning; and, most important, providing protections and encouragement to empower the widest range of specialists and citizens to participate in all levels of politics.

This is the best hope of stopping politics being dominated by PR people, party-aligned mouth pieces and industry lobbyists. In essence, the politics described in my book, and so influential in our recent election, is about freedom of speech and political activity versus those who would seek to gain by suppressing them.

More comment

Topics

New Zealand

John Key

Surveillance

Digging up dirty deeds

Nicky Hager wrote his latest book in response to what he calls the attack politics in contemporary New Zealand

THE EMPEROR'S NEW CLOTHES

The book I released in August about politics also raises important issues around journalism. It describes a dirty tricks campaign run by the New Zealand National Party to attack and smear its political opponents. Rather than the politicians standing up in parliament and fronting the attacks themselves, the book shows senior politicians using apparently independent bloggers (and some media people) to do their dirty work.

The book was based on a large leak of internal communications between the bloggers, the prime minister's office and the minister of justice – who was forced to resign shortly after the book's publication. Political journalists had long suspected links between the prime minister's office and these bloggers, but the activities were well hidden and denied. The book shows a series of attacks and manufactured scandals: researched and coordinated by government staff and then fed to journalists via the attack bloggers. It is a classic example of where a leak was crucial for the story getting out. The leak occurred early this year and I worked to get the book out before New Zealand's September 20 election.

The first issue the book raises is about the place of blogs in modern politics. I quote an internal US Republican Party presentation explaining that parties can use blogs without them needing to be "associated (in name) with your party or campaign". The presentation notes that blogs "don't have the same limitations as 'old' media", which meant the "same standards", and so are an ideal platform for discrediting opponents. It paints media as "lazy and under-informed", boasting that they frequently used stories off blogs and that blogs "often determine media content and framing". (It is an interesting document – contact me if you'd like a copy.)

This sums up the role of the two attack blogs featured in my book (Whale Oil and Kiwiblog). Year after year they attacked anyone and everyone on the public interest or left side of politics. Many hundreds of people found themselves maligned, with the apparent intention of shutting down criticism of the National government. One of the blogs is run by a former National Party president's son, the other by the National Party's chief pollster. The leaked documents prove decisively that both men were collaborating with the National Party and prime minister's staff.

Despite being blatantly partisan, both bloggers were and still are used as political commentators by the New Zealand media. This includes the party pollster, who briefs the prime minister regularly on how to manage public opinion. I think this is irresponsible of the news organisations. It's fine for commentators to be left- or right-leaning, but the public deserves to hear from people who are not extensions of a political party, government or corporate public relations campaigns. We have to do better.

The book was possibly the biggest news during the election campaign

What about the journalists who quietly took stories off the bloggers? Journalists often get stories passed to them from various sides of politics. This isn't necessarily wrong. But the book highlights the risk of being used as part of undeclared strategies. There are some terrible examples of this. A few media people – for instance one gossip columnist – appeared to be willing participants in National Party attacks. But mostly, I think, it was busy journalists being offered scoops and not thinking hard enough about what was behind them.

The book was possibly the biggest news during the election campaign. Media coverage of it was mixed. I thought many journalists pursued the issues well and kept asking questions. Some others were pathetic, acting as if I had done something wrong by raising the government's record during an election campaign. Elections, apparently, should be left to the reporting of prepared spin. There were very striking differences between news organisations in the quantity and style of coverage – interesting comparisons can be made. Also, you can tell when a news organisation is hostile towards you: they choose the most awful photographs they can!

Nonetheless, I believe that revelations such as these have a positive effect. After weeks of controversy, journalists will hopefully be on the lookout for similar activities and John Key's National Party government (which was returned to power) will be much more careful not to be caught in similar abuses of power.

As always, there were numerous ethical issues to work through with a big leak. The information came from someone who hacked the Whale Oil blog computers. My lawyer said this was a legitimate source only if there was a very high public interest. Dirty tricks and abuse of power by the prime minister's staff and minister of justice easily met this test.

But a leak like this also includes a lot of genuinely private information and so a lot of the material was not used. Further, incidental names and details were removed from the drafts. Leaks are an essential source of public information, but I believe we must also staunchly defend privacy – including unscrupulous people's privacy.

The final issue is about negative politics, which is well known to turn the general public off politics and lower the rate of voting – indeed US Republican Party strategists talk of the value of discouraging voting in certain demographics. Our recent election unsurprisingly had the second lowest turnout in our history. For anyone interested in these issues, the afterword of my book looks at what can be done in media and beyond to counter the negative effects of this style of politics.

I should warn Australian readers that the book is of course about personalities and events that are strictly from New Zealand. However, reading a case study about dirty political tactics can be a very useful way of spotting and understanding them in other contexts and countries.

If you're interested in political strategy, including the use of blogs and third-party actors, I recommend the book. You can read some chapters free at http://www.craigpotton.co.nz/flipbooks/dirty_politics/index.html.

Nicky Hager has written six books. This article is about his latest book, *Dirty Politics: How attack politics is poisoning New Zealand's political environment* (Craig Potton Publishing, Nelson, 2014)
Rod Emmerson is the editorial cartoonist for *The New Zealand Herald*

The New Zealand Herald

DJF-1

This is Exhibit DJF-1 referred to in the affidavit of David James Fisher affirmed at Auckland on 27 March 2015 before me: I Eseklelu

A (Deputy) Registrar of the High Court of New Zealand

David Fisher

David Fisher is a senior reporter for the NZ Herald.

5:30 AM Saturday Dec 1, 2012

Police checks routine work for banks

Personal information is being handed over daily without a search warrant.

Police requests for information affect Kiwibank's view of a customer. Photo / Dean Purcell

Banks get daily requests from the police for personal banking information, and one says it is influenced by law enforcement interest when it assesses customers.

The banks supply the police with information on the basis they are told that doing so assists with "maintenance of the law" - an exception in the Privacy Act to confidentiality rules.

The *Weekend Herald* has found financial information which banks promise to keep confidential is passed to police and then to other agencies.

In some cases, it ends up overseas for use in foreign court orders.

Account details, contact information and even financial information can be handed over to police without a search warrant.

The arrangement has been revealed as a result of inquiries into the Kim Dotcom case in which Kiwibank appeared to use a police request as a sign of impending trouble for the tycoon, rejecting a loan application.

The *Weekend Herald* has identified other police operations involving the same branch of police - the Organised and Financial Crime Agency of New Zealand - under which financial information about targets of interest is passed to the Ministry of Social Development and Inland Revenue.

In one case, details about a group under investigation went to Social Development which then reviewed benefits those people were receiving. In another case, financial details were passed to Inland Revenue, which then carried out a tax assessment.

Kiwibank spokesman Bruce Thompson said police requests for information influenced the bank's view of customers.

"Kiwibank takes any approach from police seriously, and as a prudent lender, would consider any such approach as part of its overall assessment of any banking relationship.

"It does not influence the bank's position one way or another but is taken into account as part of the bank's holistic assessment of a customer's character and suitability for lending or general banking services."

He said police sought information from banks on a daily basis.

A spokeswoman for the Privacy Commissioner said banks could refuse to supply the information.

"One key thing to note is that the Privacy Act provides a discretion to those agencies."

Banking Ombudsman Deborah Battell said she had not investigated any complaints about the process.

The practice is used by the police financial intelligence unit to obtain personal details without any legal compulsion or court order. It allows officers to harvest financial information by placing the decision to release information entirely on the banks.

The Banking Association's code of practice states: "We have a strict duty to protect the confidentiality of all our customers' and former customers' affairs. We are also obliged in our dealings with our personal customers to observe and comply with the Privacy Act 1993."

Police would not say how often banks gave them information.

The head of the financial crime group, Detective Superintendent Peter Devoy, said the details were being withheld because it related to

information "subject to an obligation of confidence".

It was in the public interest that such information should continue to be supplied.

A police headquarters spokeswoman said it was not an issue for the police to comment on because the decision to supply information was made by the banks.

"We lawfully obtain information for law enforcement purposes and on occasions we lawfully share information for law enforcement purposes."

Tactics employed by Ofcanz have come in for criticism in other investigations.

It is under scrutiny in the Kim Dotcom case. The search and seizure on the day of his arrest has been deemed illegal by the courts.

Cops' query hurt Dotcom loan

Kim Dotcom's application for a $4 million mortgage was declined after police asked Kiwibank for his records.

Mr Dotcom's lawyers were arranging a mortgage to buy a house next to his North Auckland mansion.

Kiwibank approved the loan then withdrew the offer just before settlement and days after police sought information on his finances.

Kiwibank spokesman Bruce Thompson said the loan was rejected after a "simple internet search" turned up troubling information. But he also said the query from the police could not be ruled out as a factor in the decision to decline the loan.

Detectives working at the FBI's behest harvested Mr Dotcom's financial information from Kiwibank, ANZ, ASB, HSBC and the BNZ, according to court records. There was no formal legal request for assistance until November 25, 2011.

In the three months before the request, according to information held at the Auckland High Court, police and the FBI met several times to discuss the internet tycoon.

Notes taken at meetings between police, Crown Law, the FBI and the GCSB by Ofcanz deputy director Detective Inspector Grant Wormald show the earliest recorded planning meeting included the head of the financial intelligence unit, Detective Superintendent Peter Devoy. The meeting on August 29, 2011 included discussion about seizing assets.

Efforts to collect the information took place through October and November 2011. The analyst who led the work, Fiona Milne, briefed US Department of Justice lead cybercrime prosecutor Jay Prabhu and FBI lead agent Michael Poston at a meeting on October 31, 2011. Notes of the meeting show she helped with a "presentation in regards to NZ financial institutions related to subjects of the investigation".

The meeting also discussed the "procedure/plan for searching financial records in NZ".

Police, FBI and Crown lawyers met again on November 4 and discussed the FBI getting an "international restraining/seizure warrant".

Police got leads on people and accounts through emails between Megaupload staff obtained on US search warrants and passed on by the FBI. Information including addresses, account numbers and account balances was handed over.

- NZ Herald

The New Zealand Herald

David Fisher
David Fisher is a senior reporter for the NZ Herald.

5:30 AM Saturday Dec 8, 2012

Banks unite in silence on giving client details to police

The ANZ, ASB Bank, BNZ and Westpac have refused to provide any information about how often they give police people's private banking information. Photo / Mark Mitchell

Banks have united to keep mum on how often they give customer details to police without a warrant.

Kiwibank has been the most open about the deal, saying it gets requests on a daily basis. It also admitted using the request as part of its "character assessment" of customers.

But ASB Bank, the ANZ, BNZ and Westpac have refused to provide any information about how often they give customer details to police.

In an industry blackout, the banking lobby group has also refused to supply the agreement it has with the police which outlines the way banks co-operate with police inquiries.

It follows the police refusal to supply details about the amount and frequency of information provided, saying the release of details might lead to a reduction in the supply of financial data.

The *Weekend Herald* uncovered the arrangement, which appears to rely on a legal loophole which allows police to gain personal financial information without going through the court process. The loophole emerged in the Kim Dotcom case where information surrendered by his banks was used in United States courts to get orders to seize assets in New Zealand.

In other cases, it has been passed to Inland Revenue and the Ministry of Social Development.

It works through police simply asking for the information while referring banks to the Privacy Act section allowing confidentiality to be waived to aid "maintenance of the law".

Privacy expert and lawyer John Edwards said the "cosy relationship" left banks exposed to potential legal action from customers.

"They wouldn't be able to say the police asked for it so that's the end of it. If Kim Dotcom wanted to make an example of them, he could cause a great deal of trouble."

He said the banks could test the request by seeking more information from police - although he doubted police would want to disclose details.

He also questioned whether banks would be qualified to judge.

Mr Edwards said the community perceived financial information to be among the most private - "second only to health information in terms of sensitivity". He said the public could take some comfort from a formal "Memorandum of Understanding" which set out the process by which information requests were managed.

The *Weekend Herald* has found an agreement exists - but neither the police nor the NZ Banking Association will make it public.

The banking association's Philip van Dyk said: "It is not a public document and we won't release it. I can't comment on the agreement."

He said he had no knowledge of what checks the banks took to make sure the law was being maintained.

The association, which touts itself as being "the industry's voice", took customer confidentiality very seriously, he said.

The Privacy Commission has said banks need to form a "reasonable belief" and simply having a request from the police might not be enough.

Green Party human rights spokeswoman Jan Logie has called on the commission to go further and has written to it urging it to reassure the public on the issue.

She said the police should be using search warrants to gain access to people's banking information.

- NZ Herald

The New Zealand Herald

David Fisher
David Fisher is a senior reporter for the NZ Herald. 11:49 AM Wednesday Mar 25, 2015

Police given personal information without search warrants

Officers obtaining personal data from range of organisations by citing clauses in legislation

Assistant Police Commissioner Malcolm Burgess. Photo / Richard Robinson

Broad swathes of people's personal data are being sought regularly by police from airlines, banks, electricity companies, internet providers and phone companies without search warrants by officers citing clauses in the Privacy Act.

Senior lawyers and the Privacy Commissioner have told the *Herald* of concerns over the practice which sees the companies voluntarily give the information to police.

Instead of seeking a legal order, police have asked companies to hand over the information to assist with the "maintenance of the law", threatened them with prosecution if they tell the person about whom they are interested and accept data with no record keeping to show how often requests are made.

The request from police carries no legal force at all yet is regularly complied with.

Production orders and search warrants, by contrast, carry a legal compulsion after being approved by a judge or senior court official.

The practice has emerged in recent cases cited by a number of lawyers and has seen a district court judge question the legal right of police to access a defendant's electricity records without a legal order because of the "increasingly intrusive nature of the information gathered by power companies".

Privacy Commissioner John Edwards said he was undertaking research to see if his office should become a central register recording the number of such requests. He said he intended to lead discussion with holders of information over how they could publicly declare the number of requests received.

"I have been concerned for some time there is not full transparency and accounting over the various means (those holding information) agencies are engaging with law enforcement agencies."

He said a range of law enforcement bodies were citing clauses in the Privacy Act to get people's personal details. Clauses in Principle 11 of the act allowed personal information to be provided if it was for "the maintenance of the law", "protection of the public revenue", to "prevent or lessen a serious threat" to inviduals and similar clauses.

But the broad intent of Principle 11 was to protect information, he said. "It is not a power to obtain information for the police."

Mr Edwards said the ability to access information quickly was understandable when time was a critical factor.

He said there was value in a public declaration by companies and others supplying information to police under the clauses. "It may well impose a greater discipline." It would mean people could "see how their information is flowing between different types of entities".

Police assistant commissioner Malcolm Burgess said "there are controls around how information is both requested and provided".

But he said there was no information held by police to show how often information was requested in this way because "there is currently no business requirement to do so".

"While the Privacy Act provisions can be used to access low level information, such as basic account details, higher level data must be obtained through a production order."

Jonathan Eaton QC provided to the Herald with an excerpt from a recent district court case in which the judge questioned whether a company surrendering a customer's electricity information without a legal order was "authorised"

271

The judge said: "Indeed, giving the increasingly intrusive nature of the information gathered by power companies, one must question whether this is material which out to be handed over without the authority of a production order."

Mr Eaton said the issue had yet to be properly tested in court and prosecutors were in danger of having evidence tossed out if it was judged to have been obtained by improper process.

He said there was also a burden of transparency on companies which held personal information. "There's a very reasonable argument they have an obligation to inform their customers."

Criminal Bar Association president Tony Bouchier said he had a client whose phone and bank records had been provided to police with "absolutely no record whatsoever that any warrants had been issued".

He said those providing information to police had an "obligation" to tell their customers they had done so.

Barrister Chris Wilkinson-Smith said a client's personal information had been provided by an airline to police under a Principle 11 clause, showing booking details, immediate and future travel plans and personal information used to make the booking.

The information was revealed by the airline - which he did not name - after police said it would help with "maintenance of the law". In this case, the person was the target of police inquiries into drug distribution.

He said he had also had cases where TradeMe provided information without any sign of legal orders.

He said police often sought search warrants to obtain information, which meant there was independent oversight.

"The danger for police is, if they don't go through the search warrant process, there could be the criticism they have taken a short cut."

Under the law the obligation to guard customers information lies with the company that holds it.

Vodafone and Air NZ were approached for information about the way they handled warrantless requests by police under the Privacy Act. Both companies said they acted in according to the law but refused further information.

A spokesman for Vodafone said questions about how often it provided information to police should be directed to police. "Where disclosure is made in response to authorities' lawful demands, our responsibility to respect our customers' right to privacy is being balanced against wider public interest considerations."

The company's "transparency report" is silent on providing information under the Privacy Act clauses even though it details search warrants and ther invasive powers available to New Zealand's intelligence agencies.

In contrast, Spark detailed the process and type of information it made available. A spokesman said concerns about the safety of people would result in call or text metadata for the last week, IP address traces, location data of where calls were made and the name and address of the account holder.

For "maintenance of the law" requests, it would tell police if the numbers were active in the last seven days and trace listed numbers to the account holder.

A spokesman said it did not keep data on the number of requests made or complied with.

TradeMe was the sole holder of information identified by the *Herald* to publicly declare the number of Principle 11 clause requests it received. Police made warrantless requests for information on 1663 occasions ending June 2014 while other government agencies made 641 requests.

- NZ Herald

272

AJB-1

This is the Exhibit marked "**AJB-1**" referred to in the affidavit of Adam Julian Boileau affirmed in Wellington on 2 April 2015 before me:

A ~~solicitor~~ barrister of the High Court of New Zealand

FROM THE PASSENGER SEAT: IT'S ONLY JUST BEGUN

by Whaleoil Staff on November 2, 2014 at 10:00am

by Pete

If you haven't yet, read Cam's 8:00am article first.

We have gone through a period where people have asked me how I can possibly be associated with "someone like" Cameron Slater. We've been quiet, taking the blows, day after day. Occasionally a post to warn people to choose which side of history they want to be on.

As with Kim Dotcom, when we told people to pick carefully, this particular story has had too many people pile on top of Cameron thinking that the guy who laughs at dead babies, calls people feral and is generally unpleasant (all extreme distortions floated by his enemies) was going down. As happens in cases like these, when people sense blood on the floor, they pile in.

Personally, I am bursting at the seams. I've been wanting to tell the story for months now. But being quiet and letting the investigations continue have paid off. We don't care who rawshark is. We've known for months. We don't care who paid him. We've known for months. The patience to stay quiet has taken some energy, and it is still not the right time to tell all.

Occasionally there have been strong warnings for people to choose which side they want to be on. This has generally been interpreted as threats. It has been interpreted as angry Cam lashing out. What we've tried to do is stop the vortex that is pulling in people that should know better, but with the available information to date, felt it was time to take an anti-Cameron stance.

Once again, people **completely** underestimate what's going on.

And, they underestimate their adversary. Cam Slater is generally considered to be a loud

mouthed boorish angry idiot with a blog where he somehow magically fools people into returning every day because of cat videos and outrageous 'shock jock' tactics.

A few, at the center of the criminal conspiracy know and fear Cam Slater for the right reasons: they know exactly what his power is. And that is why they got together to create a plan that they hoped would topple Cam Slater's will to live.

It wasn't all about Cam Slater of course, but many of the conspirators had overlapping aims. Some wanted a National government taken out. Others wanted Judith Collins taken down. But a fair proportion were busy trying to undermine the support network behind Cameron Slater. There were even commercial incentives, as media at large knew Cameron was setting up a new media company to compete for their customers.

The breadth of the conspiracy is breathtaking. It has mowed down people's careers, it's cost business, it has created reputational damage. Dimwits believing the conspirators' stories wanted nothing to do with Cam Slater and anything do with him. Thinking that being an early adopter of the righteous position was going to be just great (waves at 2 Degrees), the also piled in.

At some point people will get placed in a few boxes: those who funded it, those who broke the law, those who took the fruits of a criminal conspiracy and used it knowing it was unethical and possibly illegal, those who got together to plan to systematically tear Cameron Slater's life apart, including those who hoped Cam would do them the favour of ending his own.

We are often accused to hanging tantalising bits of information out there and then not following through. Apart from the fact that that's our prerogative, this will not be one of those occasion. But it is critical that we stick to certain rules. We can not tell you what we know, what we have hard proof of, until there is no damage to the process of justice. The reason we've been so quiet, and we will not publish everything at once, is because doing so will damage our position.

The pressure they put on Cam was otherworldly. Right now, the biggest pressure is financial. In spite of trying to keep the cost down by representing himself in various courts and inquiries, it has been heartbreaking to see Nicky Hager clock up $50k in donations on the basis of a story that was obtained by crime, based on crime, and surrounded by crime.

It is time for the "good guys" to be counted. Right now, we need our legal debts paid and some left over to deal with the remaining legal problems. The majority of these problems were caused by the people in the conspiracy, directly or indirectly. I've even found evidential links between the ongoing defamation case, the media and Nicky Hager. It shouldn't surprise me – they all have the same aim: Destroy Cam Slater.

We normally don't beg, and it is not Cam's way. But I can tell you that we're now in a position where we want to start to push back. We want to start telling the real story behind the Dirty Politics conspiracy. And we want to bring all the conspirators into the sunlight.

These people generally have access to money, we're out.

I know we've asked for your financial support to keep the blog running. I can tell you that's not under threat, in spite of the scumbags attempts to undermine its financial viability. But Cam personally is very hard hit. His closest friends have come to the end of their ability to help out.

We now come to you with the begging bowl:

> **UPDATE 11:14 am 3 Nov 2014:**
>
> **The account details here have been withdrawn and will shortly be updated. Keep your eye on a post that will be published shortly.**
>
> UPDATE: 12:21 pm – please click here for account details.

This money will not go to Cam personally. He won't be buying a tank or the latest scope for his rifle.

We need 100 people to give him $500. Out of 200,000+ readers, we need 100 of you to be part of keeping this man standing and capable of fighting back. To some degree, it's only him. And the conspiracy group contains at least one millionaire, some blogs, political parties, activists and a huge band of people that have drunk the Koolaid.

Please step up. We really need you now.

This just in

> Name: John F
>
> Email: lojofraser@gmail.com
>
> Message: Toughen up whimp and stop bleating ,and a thought your blog is an echo chamber as every one is scared of being banned like me. In concluding more power to Hager and anyone who dislikes you,thousands apon thousands

The daily barrage of trying to drag Cam's spirits down continues. The emails, comments (you don't get to see), TXT messages and facebook messages are a constant refrain telling him he is useless, his support is imaginary, and all he is doing is destroying himself and all his friends.

Time to push back.

Please help.

Tagged: blogs • criminal conspiracy • Dirty Media • Dirty Politics • msm • Nicky Hager • political parties • Rawshark • Steven Price

AJB-2

John Key: I know who Rawshark is

Published: 5:09AM Thursday October 30, 2014 Source: ONE News

John Key - Source: Breakfast

The Prime Minister claims to know who the hacker Rawshark is, an updated biography reveals today.

Mr Key claims "someone" called him and told him the real identity of the person who hacked WhaleOil blogger Cameron Slater's computer, but he decided not to try and pursue any official action over it.

"Other than having a look at this person, I thought, 'Oh well, nothing will come of it. Life goes on'," NZ Herald journalist John Roughan recounts in the revised edition of John Key: Portrait of a Prime Minister.

The biography also explains how the National Party decided ignoring Nicky Hager's book Dirty Politics, and the drip-feed of leaked emails from Rawshark, was the only possible option to survive on the campaign trail despite the media's focus on the saga.

"I thought, 'I'm not going to give him [Hager] the satisfaction of walking out of anything, not going to back away. I'm just going to talk to them every day'," Mr Key told Mr Roughan.

The Prime Minister said the "insane" demand for selfies on the campaign trail kept him confident of a strong showing on election night and said he was not surprised when the polls did not drop dramatically as some predicted.

According to the biography, the PM's staff bought five copies of Dirty Politics at the evening launch event and read through it that night, searching through "Hager's sinister insinuations for nuggets of fact involving the Prime Minister" and reported they found very few.

The book also reveals Mr Key dealt with Judith Collins by text after an email emerged alleging she had been "gunning for" the head of the Serious Fraud Office while she was Justice Minister.

Mr Key said he found out from his chief of staff on a Friday night and "decided to sleep on it".

He then texted Ms Collins saying "we need to talk" and once he had read her the details on the phone, she offered to resign and he held a press conference that day.

The first edition of John Key, Portrait of a Prime Minister, has sold more than 20,000 copies since being published at the end of June this year.

This is the Exhibit marked "**AJB-2**" referred to in the affidavit of Adam Julian Boileau affirmed in Wellington on 2 April 2015 before me:

C. a. McLaul

barrister

A ~~solicitor~~ of the High Court of New Zealand

RADIO NEW ZEALAND
TE REO IRIRANGI O AOTEAROA

This is the Exhibit marked "NAH-3" referred to in the affidavit of Nicolas Alfred Hager affirmed at Wellington on 16 June 2015 before me:

A barrister of the High Court of New Zealand

No police probe over Greens' complaint

Updated at 6:54 pm on 2 December 2014

Police will not investigate a Green Party complaint about claims in Nicky Hager's Dirty Politics book.

In the book, Mr Hager accuses the National government of feeding damaging information about their opponents to right-wing attack bloggers, such as Cameron Slater.

Listen to more on Checkpoint (3 min 58 sec)

The Greens lodged a series of complaints with the police after the book's publication, including that National staff and the then-Justice Minister Judith Collins had corruptly used information obtained in an official capacity.

Green Party co-leader Metiria Turei.
Photo: RNZ / Diego Opatowski

They also complained about allegations of blackmail against former ACT Party leader Rodney Hide.

Police have since reviewed the allegations and say they appear to fall short of criminal offending.

However, they are still considering a complaint, lodged by both Labour and the Greens, that National staff unlawfully accessed sensitive information on Labour's website in 2011.

The police say if they do decide to investigate, it will be under Labour's complaint.

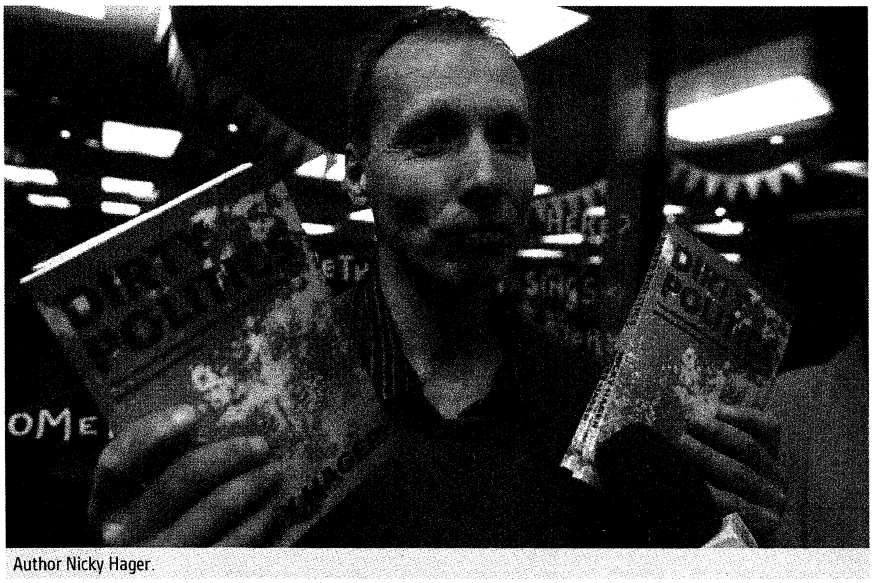
Green Party's co-leader Metiria Turei said the police inaction is wrong and smacked of a "double standard."

"They were quick to take Cameron Slater's complaint seriously and raid Nicky Hager's house, but sat on our complaint for months ... We need the police to act fairly, and I have real questions as to whether they have in this instance."

The police [http://www.radionz.co.nz/news/national/256277/author-nicky-hager's-home-raided raided Nicky Hager's home] in October in response to a complaint from Mr Slater about the alleged hacking of his emails which were used in Dirty Politics.

Ms Turei says there is more than enough evidence to warrant an investigation into the claims in the book.

"We would be very concerned if the Police are applying different thresholds for launching criminal investigations depending on what side of politics you come from."



Author Nicky Hager.

Photo: RNZ / Diego Opatowski

Related

- Advice sought on PM destroying texts
- PM's contact with blogger questioned
- John Key refuses to accept Slater link
- Report slams SIS over info release
- Labour wants apology from PM

Next story in Political: Anti-terror bill changes win Labour support

National

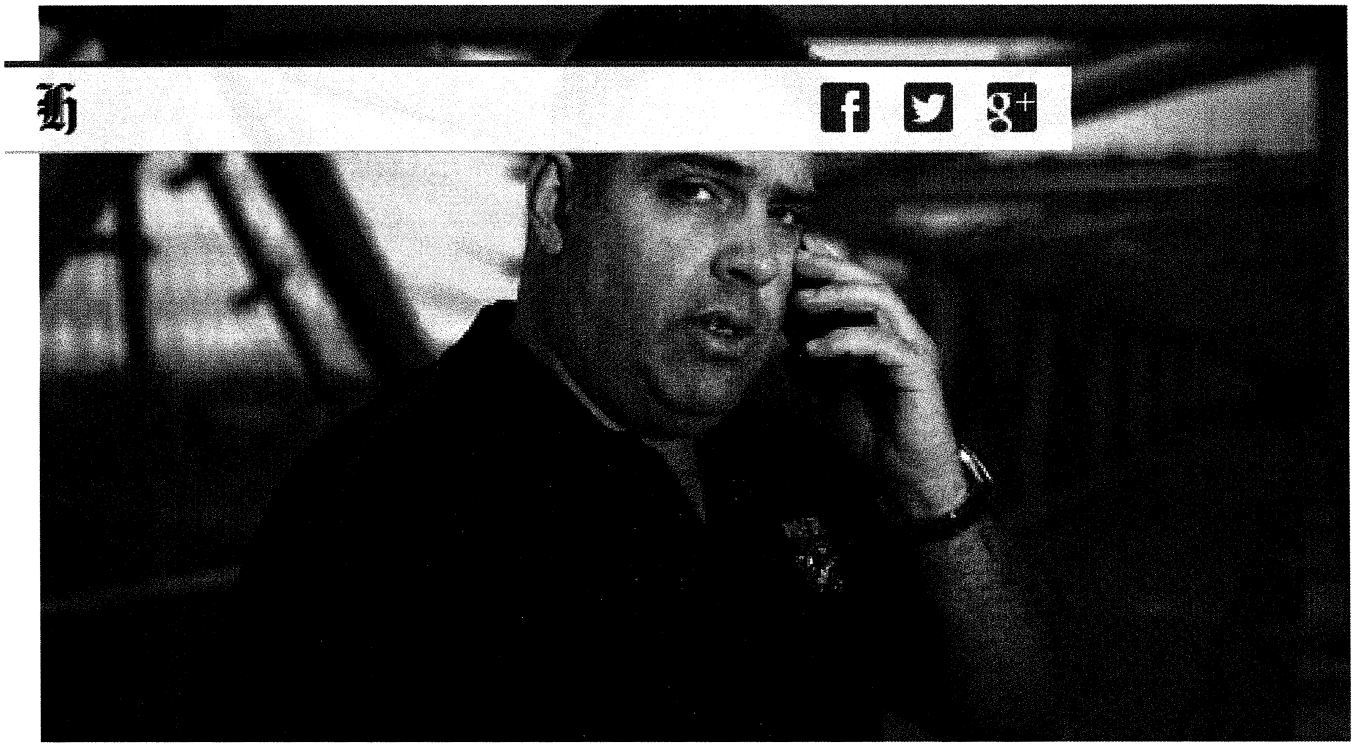
This is the Exhibit marked "NAH-4" referred to in the affidavit of Nicolas Alfred Hager affirmed at Wellington on 16 June 2015 before me:

A barrister of the High Court of New Zealand

Patrice Dougan
Patrice Dougan is a NZME. News Service reporter based in Auckland.

Blogger accused of paying hacker

Saturday, 06 June 2015



Cameron Slater, publisher of the Whale Oil Beef Hooked blog takes a phone call during a portrait session at Viaduct Harbour on September 12, 2014 in Auckland. Photo / Phil Walter, Getty Images

By Patrice Dougan

Right-wing blogger Cameron Slater has been accused of paying a man to hack into an opposition website for political gain.

In a statement provided to NZME. News Service, police confirmed they were investigating the claims, saying they had "received a complaint regarding an alleged attempt to procure the hacking of a computer system".

"The complaint is being investigated by Counties Manukau CIB," the statement said.

"There are a number of complexities to the investigation, including the posting online of documentation which has already compromised the investigation and is making our inquires more difficult.

"Police are taking a cautious approach, and working through a number of complex steps to gather the necessary information to advance the enquiry.

"Any decision on charges is some way off at this stage, and will be made after a thorough assessment of all relevant information."

The controversial and outspoken political commentator denies the claims, but police have reportedly confirmed they are investigating the allegations made by Ben Rachinger.

The IT consultant posted his claims on the internet earlier this year, and this morning The Nation broadcast an interview with him, detailing his claims Slater commissioned him to hack into left-wing political blog The Standard to try to uncover the identities of the authors of blogs written anonymously or under pseudonyms.

"Cameron Slater asked me, for financial benefit, to hack into The Standard website and to pull out any and all information about authors of anonymous blog posts on The Standard and also to find out email addresses and IP addresses for further hacking," Mr Rachinger told TV's The Nation.

Slater has long claimed blogs on The Standard are ghost written by Labour insiders, including staff members.

In an encrypted text sent to Mr Rachinger in January, Slater allegedly said: "I want proof of admin at The Standard ... I will destroy them."

He later allegedly said: "I want them all outed, all the MPs, [The Standard founder Lynn] Prentice, [Labour Party chief of staff Matt] McCarten ... all of them."

Mr Rachinger says Slater asked him to "focus on this job of getting into The Standard", and said he had $5000 available to pay him to do so. But Slater would not name his backer, who was funding the hacking request.

Mr Rachinger says he became Slater's confidant after the IT consultant got in touch with the blogger after a cyber attack on his WhaleOil site. Hacked emails stolen during the security breach were later used to form the information for journalist Nicky Hager's Dirty Politics book, which was released before last year's election.

Mr Rachinger said he offered to strengthen the security on Slater's website, and they continued to stay in touch.

Slater wanted to get back at those who had criticised him in the fall-out from Dirty Politics, Mr Rachinger said. Initially he wanted Mr Rachinger to out 'Rawshark', the hacker who claimed responsibility for the attack on WhaleOil. But then focussed on targeting The Standard.

"His plan was to use this information to hit back at the Labour Party, and specifically [Labour leader] Andrew Little, on the first day of Parliament, in order to dampen the affects of Dirty Politics the year before," Mr Rachinger said.

Bank records showed Mr Rachinger received numerous payments from Slater's company Social Media Co, totalling $9100 over a period of three months.

In the emails and text messages seen by The Nation, Mr Rachinger claimed to be "in" The Standard's system and getting the information, but Mr Rachinger told the programme that he never actually hacked the website, and was simply bluffing Slater.

"I did not have that information at that stage, that information was a bluff. Any information I provided to him was publicly accessible from Google or just looking through websites on the surface," he said.

Mr Rachinger said he was attempting to carry out "an ad hoc investigation of my own".

"I believed I would be able to get the evidence that I thought I required to shine sunlight on Mr Slater and his funder's activities."

Their relationship turned sour when Slater realised he'd paid Mr Rachinger and received little in return, the show claimed.

281

In text messages Slater allegedly sent to Mr Rachinger, he said he has "nothing after $4k", claiming Mr Rachinger has defrauded him, and claiming he was "angry as f***".

In one message he allegedly said: "It's no small thing I'm doing this, I could be being set up in a sting by a media person or cops."

The Nation said police had confirmed that detectives at the Counties Manukau CIB were investigating an allegation that Slater offered money in a bid to procure the hacking of a computer system.

Police said it was a complex investigation and they're still gathering all the necessary information, the programme said. Any decision on charges would be some way off.

Slater declined to be interviewed or provide a statement to The Nation, but "unequivocally denied" the claims, the show said.

He told the programme Mr Rachinger approached him with the information, offering it up for a price.

In an audio clip from a phonecall to Slater, he said he was "sick to death of people trying to set me up".

"I don't break the law, that's the end of the story."

Related Content

Political roundup: A Green surprise

James who? That'd be the likely response from many if the Green Party go for the bold option of electing a relatively unknown candidate as their new male ...

Political roundup: Dirty Politics 'done dirt cheap'

We can expect hacking, privacy and surveillance issues to be central to the way the political system works in this country, writes Bryce Edwards.

Share this article

More National

- Kauri exports make mockery of law - conservationists
- Bottom-trawling banned from area off West Coast
- Raw: Police storm Chch properties in drug crackdown
- Kumar trial: Teen 'lived in a drug house'
- Jewellery thief admits hammer attack
- Three charged over metal barrier death

The New Zealand Herald

Assembled by: (dynamic) on production bpcf03 at 16 Jun 2015 13:35:19 Processing Time: 656ms

DJF-2

This is Exhibit DJF-2 referred to in the affidavit of David James Fisher affirmed at Auckland on 16 June 2015 before me:

A (Deputy) Registrar of the DISTRICT COURT ~~High Court~~ of New Zealand

Lorna Perkins
Deputy Registrar

Natalie Akoorie
Natalie Akoorie is a reporter at the NZ Herald based in Hamilton.

No charges likely for burglar who found body

Horrified, screaming intruder phones police after coming upon hanging victim.

11:30 AM Thursday Jun 20, 2013

Inspector Greg Nicholls. Photo / Sarah Ivey

A burglar who discovered a dead body hanging in a Hamilton house is unlikely to face charges for the break-in.

The 26-year-old man made the grisly discovery early yesterday morning while attempting to burgle the vacant house in the suburb of Fairfield.

Hamilton Police city tactical coordinator Senior Sergeant Freda Grace said the burglar, who called police himself to raise the alarm, had been arrested but not charged.

Mrs Grace said the man was released after helping police with their inquiries.

The incident unfolded in the early hours of yesterday morning when the burglar stumbled across the dead body hanging in the dark.

His screams alerted neighbours who also phoned police. It's understood they thought the screaming was a domestic dispute.

Mrs Grace said the victim had died hours before the burglary but if not for the break-in he may not have been found for days.

She said the death of the man, whose age is unknown, was not being treated as suspicious and had been referred to the coroner.

The burglar was known to police and Mrs Grace hoped the "weird" circumstances would alter his behaviour.

"Hopefully there will be a positive out of it and that he will decide it's not the thing to do. I would be taking that as pretty bad karma."

Mrs Grace said the whole situation was incredibly sad".

"It's sad for the guy who felt so bad that that's what happened to him. Really the whole set of circumstancas are just horrid."

She did not know if the dead man's next of kin had been notified.

- NZ Herald

This is the annexure marked DJF-2
referred to in the within affidavit of
DAVID JAMES FISHER
sworn at Auckland this 18th
day of JUNE 2015
Deputy Registrar, District Court, Auckland

Lorna Perkins
Deputy Registrar

AJB-3

This is Exhibit AJB-3 referred to in the affidavit of Adam Julian Boileau affirmed at Wellington on 16 June 2015 before me:

A barrister of the High Court of New Zealand

About

amnesia, *noun*:
forgetfulness; loss of long-term memory.

incognito, *adjective & adverb*:
(of a person) having one's true identity concealed.

Download
Tails 1.4
May 12, 2015

About
Getting started...
Documentation
Help & Support
Contribute
News

Donate

Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it to explicitly.

It is a complete operating system designed to be used from a DVD, USB stick, or SD card independently of the computer's

original operating system. It is Free Software and based on Debian GNU/Linux .

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc.

Online anonymity and censorship circumvention

Tor

Tails relies on the Tor anonymity network to protect your privacy online:

- all software is configured to connect to the Internet through Tor
- if an application tries to connect to the Internet directly, the connection is automatically blocked for security.

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Using Tor you can:

- be anonymous online by hiding your location,
- connect to services that would be censored otherwise;
- resist attacks that block the usage of Tor using circumvention tools such as bridges.

To learn more about Tor, see the official Tor website :

- Tor overview: Why we need Tor
- Tor overview: How does Tor work
- Who uses Tor?
- Understanding and Using Tor — An Introduction for the Layman

To learn more about how the usage of Tor is enforced, see our design document.

I2P

You can also use Tails to access I2P which is an anonymity network different from Tor.

Learn how to use I2P in Tails in the documentation.

To know how I2P is implemented in Tails, see our design document.

Use anywhere but leave no trace

287

Using Tails on a computer doesn't alter or depend on the operating system installed on it. So you can use it in the same way on your computer, a friend's or one at your local library. After shutting down Tails, the computer can start again on its usual operating system.

Tails is configured with special care to not use the computer's hard-disks, even if there is some swap space on them. The only storage space used by Tails is the RAM, which is automatically erased when the computer shuts down. So you won't leave any trace neither of the Tails system nor of what you did on the computer. That's why we call it "amnesic".

This allows you to work on sensitive documents on any computer and protect you from data recovery after shutdown. Of course, you can still explicitly save some documents to another USB or external hard-disk and take them away for future use.

State-of-the-art cryptographic tools

Tails also comes with a selection of tools to protect your data using strong encryption:

- Encrypt your USB sticks or external hard-disks using LUKS+, the Linux standard for disk-encryption.
- Automatically encrypt with HTTPS all your communications to a number of major websites using HTTPS Everywhere , a Firefox extension developed by the Electronic Frontier Foundation .
- Encrypt and sign your emails and documents using the *de facto* standard OpenPGP+ either from Tails email client, text editor or file browser.
- Protect your instant messaging conversations using OTR+, a cryptographic tool that provides encryption, authentication

and deniability.

- Securely delete your files and clean your diskspace using Nautilus Wipe .

Read more about those tools in the documentation.

What's next?

To continue discovering Tails, you can now read:

- the warning page to understand better the security limitations of Tails and Tor,
- more details about the features and software included in Tails,
- our documentation explaining in detail how to use Tails,
- some hints on why should you trust Tails,
- our design document about Tails specification, threat model and implementation,
- the calendar holds the release dates, meetings and other events.

Press and media

See Press and media information.

Acknowledgments and similar projects

See Acknowledgments and similar projects.

Last edited Fri 13 Mar 2015 04:25:39 PM CET

"A"

Brent Whale, CFCE, CAWFE, EnCE

This is the document marked with "A" referred to in the annexed affidavit of BRENT PETER WHALE sworn at Auckland this 1 day of May 2015 before me:

A Solicitor of the High Court of New Zealand

Brent Whale

Brent Whale is the director of Computer Forensic Solutions Ltd, which specialises in computer and mobile phone forensic investigations.

Following a twenty-two year career with the New Zealand Customs Service, Brent brought his skills and experience into the private sector in January 2007.

Capabilities include Computer forensic analysis and investigation, and mobile phone examinations. Brent is also a certified trainer in computer forensics. He has been involved in delivering computer forensic training in South East Asia as well as the USA, Germany and Croatia.

A brief *c.v.* is included below.

Relevant Employment:

2007 – 2015	Director, Computer Forensic Solutions Ltd.
1984 – 2007	Customs Officer, NZ Customs Service
2000 – 2007	Head of the Electronic Forensic Unit
1996 – 2000	Customs Investigator
1990 – 1996	Border Inspector
1988 – 1990	Drug Intelligence (NZ Police Nat. H.Q.)
1986 – 1988	Border Protection Officer

Relevant Qualifications:

Certified Advanced Windows Forensic Examiner (CAWFE) 2012.
Certified Forensic Computer Examiner (CFCE), 2002, re-certifications are current.
EnCase Certified Computer Examiner (EnCE), 2004, re-certifications are current.
CompTIA A+ certification, 2000

Courses Completed:

International Association of Computer Investigative Specialists (IACIS)
Basic Computer Forensic Examiner (Florida USA), 2001
Advanced Computer Forensics (Florida USA), 2002
Advanced Windows Forensic Examination (Brisbane Australia), 2010

National White Collar Crime Centre (NW3C)
Basic Data Recovery and Analysis (NY, USA) 2002
Advanced Data Recovery and Analysis (WV, USA) 2002

Guidance Software Inc.
EnCase (Auckland, NZ) 1999
EnCase Advanced Internet Examinations (Auckland, NZ) 2005

Access Data
Intermediate Computer Forensics (Sydney, AUL) 2003

Micro Systemation
Mobile Phone Examination (Melbourne, AUL) 2008

Sumuri
Macintosh Forensic training (Auckland, NZ) 2010

Instructing experience:

IACIS (Florida, USA) 2003 - 2005, 2007 - 2011
Interpol (Lyons, France) 2003
Forensic Methodology (Malaca, Malaysia) 2007
IACIS (Germany) 2007 - 2008
IACIS Cellphone forensics (Germany) 2009
IACIS (Croatia) 2013

Publications:

IACIS Computer Forensics Manual (contributing) 2003 - 2008

Voluntary Positions:

IACIS – Director of Standards 2011 - 2015
Internet Safety Group (ISG) 2004 - 2009