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 1: Applicant's affidavits

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

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*

Affidavit of Nicolas Alfred Hager

Affirmed: 2 April 2015

Solicitor
Thomas Bennion
Bennion Law
L1, 181 Cuba Street
PO Box 25 433
Wellington 6146
Tel: +64 4 473 5755
Fax: +64 4 381 3276
tom@bennion.co.nz

Counsel
Julian Miles QC
Richmond Chambers
L5, General Buildings
33 Shortland Street
PO Box 1008
Auckland 1140
Tel: + 64 9 600 5504
miles@richmondchambers.co.nz

Felix Geiringer
Terrace Chambers
No. 1 The Terrace
PO Box 10 201
Wellington 6143
Tel: +64 4 909 7297
Fax: +64 4 909 7298
felix.geiringer@terracechambers.co.nz

I, Nicolas Alfred Hager, investigative journalist of Wellington, solemnly and sincerely affirm:

Introduction

1. I am the applicant in these proceedings. I make this affidavit to set out the factual basis of my claim for review.

My work

Overview

2. Since the early 1990s, I have worked as an investigative journalist and author. I have written six books and various investigative feature articles for New Zealand and overseas publication. I work independently, publishing in newspapers on a freelance basis.

3. I have specialised in investigating complex and/or actively hidden subjects that typically take months or years of research. The subjects have included intelligence agencies, military, Police, environment, health, the public relations industry, and unethical or undemocratic parts of politics. There are common themes in this work relating to democracy, integrity in government, transparency, freedom of information and respect for human rights. Most of my work has been in these areas.

My books

Secret Power

4. My first book was called *Secret Power, New Zealand's role in the international intelligence network*, published by Craig Potton Publishing in 1996. The book was the product of several years of research into the previously little-known Government Communications Security Bureau (the "**GCSB**"). The GCSB is a New Zealand foreign intelligence agency. The book described the agency's history, internal structures, operations, training, and facilities.

5. The book described long-term GCSB operations against most South Pacific nations, Japan, Russia, and many other countries. Its most important

finding concerned GCSB participation in a US-UK-Canada-Australia-New Zealand global surveillance system called Echelon, the antecedent of the mass surveillance systems revealed in recent years by the US whistle-blower Edward Snowden. This was the first detailed description of the Echelon system to be published. It included my research documenting a world-wide network of allied intelligence bases that made up the Echelon system.

6. The following year, in 1997, I wrote an article on the workings of the Echelon system in a United States intelligence periodical called Covert Action Quarterly ("Exposing the Global Surveillance System", Covert Action Quarterly, 1 February 1997) . This article was highlighted in a European Parliament report about surveillance and privacy issues in February 1998 (Directorate General for Research, "An appraisal of technologies of political control", 22 February 1998). During the following three years there was debate in several European parliaments about Echelon and there were hundreds of news stories and documentaries on the subject.

7. In 2000-01 there was a year-long special inquiry into Echelon by the European Parliament, the Temporary Committee on the Echelon Interception System (final report 11 July 2001, adopted by European parliament 5 September 2011). I was invited to present to the committee in 2001 and advised on its recommendations. I have been interviewed many times by international media and spoken at overseas conferences on this subject since. *Secret Power* has been translated into various other languages.

8. Former Prime Minister David Lange wrote a foreword to the book in which he said that "an astonishing number of people have told him things that I, as Prime Minister in charge of the intelligence services, was never told." He wrote "it is an outrage that I and other ministers were told so little, and this raises the question of to whom those concerned saw themselves ultimately responsible".

9. The international reaction to this book encouraged me to specialise full time in investigative journalism.

10. My research into the GCSB and international surveillance systems was based primarily on information provided by confidential sources. It would have been impossible to gather the information without those confidential sources. I approached a series of past and present intelligence officers and invited them to assist me to inform the public about these intelligence activities. I assured them that I would never reveal their identities nor risk identifying them by what I wrote.

11. Many of the sources had never talked to their families or friends about their jobs and so a high degree of trust and care was required to work with them. None of the sources have ever been found out. To the best of my knowledge, none were suspected or questioned.

12. In each case, the confidential sources knew that I was seeking this information for the purpose of publishing news stories – either in the form of a book or a newspaper article – in order to convey that information to the public as part of a coherent story. I am always open with my sources as to why I am seeking the information. I do not engage in surreptitious practices designed to trick people into sharing confidential information.

Secrets and Lies

13. My second book was about the public relations industry. It was called *Secrets and Lies, The anatomy of an anti-environmental PR campaign*. The book was co-authored with Bob Burton and published by Craig Potton publishing in 1999. Its subject was the growing trend for controversial industries to use public relations companies to attempt to silence or marginalise their critics. The book focussed on a US public relations company employed by a New Zealand state-owned enterprise to combat environmental groups that opposed continued logging of native forests on New Zealand's West Coast.

A12 · NH

004

14. The book documented a set of aggressive tactics including infiltration of environmental groups, pressure applied to the environmental groups' funders, orchestrated pressure on scientists and ecologists who gave evidence against the logging, a fake pro-logging community group, and other underhand tactics. The underlying theme of the book was about transparency of government organisations and protection of freedom of speech.

15. The revelations in the book included details of the state-owned enterprise (Timberlands West Coast Limited) and its PR advisors trying to manipulate forestry policy in the Labour Party. These and the other revelations helped lead to the Labour Government ending all logging of publicly-owned native forests on the West Coast. The book was also published in the United States, where there was interest in documenting this type of public relations campaign.

16. The activities described in the book had been deliberately kept secret and, when suspected by journalists, had been denied. It is unlikely that the activities would have ever been publicised if I had not been leaked information and documents by insiders who were unhappy about the unethical tactics. The documents included PR strategy plans, PR teleconference minutes, and other undeniable source materials.

17. The information and documents were provided to me by a range of confidential sources who contributed different parts of the story. This information was provided on the strict understanding that I would keep their identities confidential permanently. As above, the confidential sources all knew what I intended to do with the information they provided. And, as above, none of their identities have ever been revealed.

Seeds of Distrust

18. My third book was called *Seeds of Distrust, The story of a GE cover-up*. It was published in 2002 by Craig Potton Publishing. Unlike the previous two

books, where I had been researching the subjects and sought the sources myself, in this case a confidential source offered me the information.

19. The story concerned an accidental release of genetically-engineered corn plants, as probable contamination in a shipment of normal corn seeds which was then planted out in New Zealand. The Labour-led government initially prepared to have the crops destroyed. This was because the GE plants, as new organisms, were unlawful and threatened New Zealand trade in some markets. However, international seed company lobbying led to the government temporarily introducing a policy of accepting a low level of GE corn contamination. This allowed the crops to be harvested, and for the whole incident to be kept secret. I felt that this was a case study of industry lobbying, weak government processes and secrecy allowing a government to act differently than it would if its actions were visible to the public.

20. The public servant who brought me the story was unhappy about the rules being bent and the active efforts employed to keep the issue secret. The source was aware of my previous work. The source's intention in coming to me was to have the story told to the public through a news publication. However, in order to agree to provide that information to me the source needed me to guarantee that I would not reveal the source's identity.

21. I was provided with documents showing each stage of the unpublicised contamination crisis. I could use only a fraction of these documents because of my obligation to protect the source's identity. Most of them had an extremely limited circulation and could have cast suspicion on my source.

22. I had worked at the Department of Scientific and Industrial Research earlier in my career. This meant I was able to contact a range of other sources with knowledge of the events and issues. I strictly undertook to protect the identity of these sources as well. This enabled me to corroborate the information I had obtained and to fill in blanks in the story.

NH

AAA

23. The government publicly denied everything in the book. However, the head of the Ministry for the Environment conceded to media that the book was "largely accurate" (Barry Carbon, in Guy MacGibbon, "Hager's Facts Fine - Environment Ministry CEO", Scoop, 11 July 2002). A select committee was formed to inquiry into the scandal. However, the Committee's chairperson complained that it had been obstructed from completing its investigation. When the Committee reported back in 2004, it was divided on the issue of the accuracy of the matters set out in *Seeds of Distrust*. All of the National Party members of that committee were of the view that the book was accurate ("Inquiry into the alleged accidental release of genetically engineered sweet corn plants in 2000 and the subsequent actions taken", New Zealand House of Representatives, October 20014).

24. As a result of the book, the government tightened its rules for handling genetically-engineered organisms. By chance, only weeks after the book's publication more corn crops were found that were contaminated with genetically-engineered corn plants. The officials and government immediately announced the incident and kept the public informed as they investigated the case and then destroyed the affected crops. New Zealand continues to have strict biosecurity rules covering introduction of unapproved new organisms.

The Hollow Men

25. My fourth book was published by Craig Potton Publishing in 2006 and concerned transparency and ethics in politics. It was called *The Hollow Men, A study in the politics of deception*. The book was a three-year history of the National Party leader's office during the leadership of Don Brash, including the 2005 election campaign.

26. The book began with the inside story of National Party's secret relations with the Exclusive Brethren church. The Exclusive Brethren had collaborated with National Party staff to provide over a million dollars of undeclared election advertising attacking National's political opponents.

CAA 007

National and Don Brash had denied any links to the Exclusive Brethren. Documents quoted in the book provided evidence that this was untrue.

27. The main part of the book concerned political tactics used to boost Mr Brash's popularity, including the conscious use of racism and denigration of beneficiaries. It also gave the identity of the main party donors whose identities and motives had been kept secret. The objective of the book was to document unethical tactics and discuss the lines between ethical and unethical ways of doing politics. The book showed how the politicians acted and spoke when they were confident of not being found out, and thus the gap between manufactured appearances and reality in politics. It is also about the unseen role of political advisors. The book is now used as a resource by various university politics courses.

28. Many of the events documented in the book had been actively kept secret and could not have been written about without confidential sources. The book was based on interviews with party insiders and a large number of inside documents: strategy plans, e-mails between the leader's office staff and leader, itineraries and so on. I assured each confidential source that I would protect their identity as an essential part of securing their cooperation. As always, they understood what I intended to do with the information provided, and their identities have never been revealed.

29. There would probably have been no political accountability for the politicians and their staffs without the confidential sources. As it turned out, Don Brash resigned as National Party leader on the day of the book's release and a few days later resigned from Parliament. This appeared to be influenced by information provided by the sources that contradicted public statements he had made during the 2005 election campaign about his links to the Exclusive Brethren. Various of his political staff left Parliament at that time as well. The following party leader, John Key, distanced himself from various tactics used by Brash and his advisors, notably the use of race.

30. Former National Party MP Marilyn Waring wrote in the foreword that she remembered the events discussed in the book "but no one has ever held

them up to the light, and it is time that this happened, so that New Zealanders can decide the nature of the democracy that they want.... It is my hope that the ultimate effect of *The Hollow Men* will be the return of honour and honesty to our democracy."

31. The New Zealand Herald wrote on 31 December 2009 that *The Hollow Men* was one of the "top ten [New Zealand] books of the decade." The book was adapted into a feature-length documentary and an award-winning stage play both with the same title.

Other People's Wars

32. My fifth book was published in 2011 by Craig Potton Publishing. It was called *Other People's Wars, New Zealand in Afghanistan, Iraq, and the war on terror*. This book had taken several years of work, gradually piecing together the history of ten years of New Zealand military and intelligence involvement in Afghanistan and Iraq.

33. My motive for writing the book was that this was New Zealand's longest overseas war, but it seemed to me that most of the stories had remained hidden from the public. I had also written several newspaper features on the subject, but the book set out to be a fuller record of this piece of history. The book revealed admirable parts of New Zealand's roles and ones that the authorities were embarrassed about and kept secret.

34. There were also various clear examples of the military failing to follow the government's instructions, raising issues of civilian control of the military. An underlying theme of the book was the difference between the view of the war provided by New Zealand and allied military public relations and the reality.

35. I write my books with extensive endnotes so that readers and other researchers can know the basis for each piece of information. *Other People's Wars* has about 1400 individual endnotes, each referencing one or more documents, articles and other sources.

NH

CAA 009

36. The book is now used as a reference book by students in universities and military studies courses. It has been used as a model for similar studies in other countries, notably Germany and Italy. The book was adapted into a stage play with the same title. In 2015, Penguin Books requested rights to use an extract from the book in its forthcoming book *The Penguin Book of New Zealand War Writing*, by Harry Ricketts and Gavin McLean.

37. Most information in the book had never been published before. The book was only possible because I interviewed a wide range of past and current military and intelligence staff about their experiences. I was also provided with thousands of internal documents. In seeking that information, I was open with those I spoke to about the fact that I was a journalist investigating these matters for the purpose of writing news stories.

38. None of these military and intelligence personnel would have taken part in the research without my assurance that I would strictly protect their identity. None has been identified. Many told me that they could not continue to work in that field, and would be alienated from their past or present colleagues, if it was known that they had helped me with the book. However they felt that if they could participate confidentially, the public had a right to know what the military and intelligence agencies were doing on its behalf.

39. I had to make numerous decisions about which leaked information should be included or not included in this and the other books. There were many documents and details that I did not include because they did not have sufficient public interest or where privacy or security needed to come first.

My articles

40. I also write investigative articles. Some of my research projects end up suiting book-length publication while others suit feature article publication. In New Zealand, I have mostly written in the Sunday Star-Times. I have also written in the Otago Daily Times, Christchurch Press, the New Zealand Herald, the New Zealand Listener, the Scoop news website, and

SAH · NH 010

the Pundit blogsite. All of these publications disseminate news and observations on news to the public. The articles have covered a wide range of subjects. Some examples follow.

41. In 2005, I wrote two articles in the Sunday Star-Times revealing that two men caught by Police procuring a false New Zealand passport the year before were long-term employees of the Israeli intelligence agency Mossad. The article, which relied on confidential overseas intelligence sources, detailed the men's careers in Mossad and an earlier failed intelligence operation of which one had been in charge. ("Mossad man's history of bungles" and "Australians aware of agent's connections to Mossad", Sunday Star-Times, 27 February 2005).

42. In 2007, I wrote an article in the Sunday Star-Times about the state-owned coal company Solid Energy paying private investigators to infiltrate and report on environmental groups concerned about climate change. The articles, which relied on confidential sources, led to the minister in charge of state-owned enterprises instructing Solid Energy to stop these activities. ("I was paid to betray protesters", Sunday Star-Times, 27 May 2007.)

43. In 2008, I wrote a major feature in the Sunday Star-Times entitled 'Private hospitals will 'cream off' easiest work under Nat scheme", which described changes being made to the New Zealand health system. These changes had been occurring without publicity and the article helped prompt public debate on the policies. I was assisted in researching this article by confidential sources in the health sector, who had been warned by their employers that they should not talk about the policy changes with the media. I had to assure these people that their identities would be protected. ("Private hospitals will 'cream off' easiest work under Nat scheme", Sunday Star-Times, 12 October 2008.)

44. I have written a series of articles about cases where New Zealand Police appeared to be trespassing too far onto personal and political rights. In 2008, I wrote a front-page exposé in the Sunday Star-Times about a man who had been employed by Police for the previous ten years to infiltrate

political groups including environmental groups, animal welfare groups and peace groups. The man had had long-term relationships with women in the groups, had proposed and helped plan protests, and investigated the personal lives of key individuals, all while reporting to his Police handlers. The investigation involved gaining the trust of a range of non-government sources, many of whom only spoke to me on the condition of confidentiality. ("Crossing the line: the activist who became Police informer" and "Police anti-terror group spies on protest groups", Sunday Star-Times, 14 December 2008; "Activist considers court actions against Police informer", Sunday Star-Times, 21 December 2008.)

45. In 2010, I wrote articles in the Sunday Star-Times about New Zealand telecommunications companies that were installing "interception capable" equipment into all their networks. Confidential sources in the companies described the new equipment. I had written an earlier article in the Sunday Star-Times in the year 2000 about US Federal Bureau of Investigations lobbying of countries around the world to introduce these interception capable systems, predicting that New Zealand would eventually introduce the same laws and systems. Ten years later the confidential sources allowed me to inform the New Zealand public that the interception systems had been introduced in this country. ("NZ's cyber spies win new powers" and "FBI role in Big Brother's sharper eyes, ears", Sunday Star-Times, 3 January 2010.)

46. My largest investigative project in 2012-2013 was about people and companies that hide their assets and business activities in tax havens. I worked as part of a team of investigative journalists, the other main members being in Romania, Britain, Russia, the United States, Costa Rica, and Sweden. We had been given a large leak of internal tax haven information and spent over a year studying the data, and researching and verifying stories. The project was called "Offshore Leaks". The data revealed questionable tax haven activities of dictators, senior politicians, major businesses, criminals, and many others. In addition to the leaked

NA
AA 012

data, I found and worked with a number of confidential sources to verify and build the stories. This research resulted in a series of articles in New Zealand and other countries in 2013.

47. One of my stories described Indonesian "crony" billionaires who had been given immense public resources during the Suharto regime years and moved them into tax havens to avoid having to repay the money when democracy was restored. Other subjects I covered were Indonesian billionaires shifting their business activities to tax havens to avoid tax, and medical professionals who were paid large sums into tax haven bank accounts by pharmaceutical companies. The European Commissioner for Taxation, Algirdas Semeta, issued a press statement saying "Recent developments, fuelled by the outcome of the Offshore Leaks, confirm the urgency for more and better action against tax evasion.... I hope to see rapid adoption of our proposals for a stronger EU stance against tax fraud" (Statement by Commissioner Semeta on fighting tax evasion, Brussels, 8 April 2013.)

48. The tax haven project occurred under the auspices of a Washington DC-based organisation called the International Consortium of Investigative Journalists ("ICIJ"). This organisation coordinates multi-country investigations on high public interest subjects. I have been the New Zealand representative of the ICIJ since 2002. On the tax haven project I was one of three people who coordinated 86 journalists in 46 countries who were researching and writing stories on the tax haven information. These stories appeared on the website of the ICIJ and in newspapers around the world.

49. I have also written in overseas publications including Le Monde Diplomatique, a monthly newspaper published in France, the Guardian in Britain, Suddeutsche Zeitung in Germany, Ta Nea in Greece, l'Espresso in Italy, and Covert Action Quarterly in the United States of America.

50. In 2010, for instance, I wrote an article in Le Monde Diplomatique about a large and previously unknown Israeli intelligence base used to spy on West

European countries and the Middle East. This article was based on confidential sources, whom I had assured would not be identified. I did not include most of the information I had been given by the sources as it risked showing when and in what way they had been involved with the facility.

51. In 2014, following publication of the book *Dirty Politics*, I wrote articles on the same subject based on the same research and materials. I wrote in the British Guardian newspaper ("New Zealand elections: dirty tricks helped John Key win another term", Guardian, 24 September 2014) and Australian Walkley Magazine ("Digging up dirty deeds", Walkley Magazine, October 2014). True copies of those articles are attached to this affidavit and are marked as Exhibits "**NAH-1**".

52. In 2015, I worked in collaboration with the US-based Intercept news organisation and the New Zealand Herald to research and publish a series of stories about New Zealand's intelligence activities using documents obtained by US intelligence whistle-blower Edward Snowden and other sources. A story in the New Zealand Herald on 23 March 2015, for instance, described the government using the GCSB to help Cabinet colleague Tim Groser's bid to get the job of director general of the World Trade Organisation by monitoring email communications of and about his eight competitors for the job ("How spy agency homed in on Groser's rivals", New Zealand Herald, 23 March 2015). While the source of the Snowden documents is obviously known, I sought and worked with several confidential sources to confirm and develop the stories.

53. In every case where I describe people as being confidential informants it is because they were providing me with information, understanding that I was intended to publish it as part of a news story, on the grounds that I expressly promised that I would keep their identities secret.

NH
NAH · 014

Future work

54. My current and intended future work is a continuation of what I have been doing for these last twenty odd years. I am still investigating news stories in relation to my main areas of interest. Those news stories are still reliant on information from confidential sources. And it is my intention, as known by those confidential sources, to use that information as part of stories that are going to be published in a similar way to my past stories – either as books or as articles depending on the circumstances.

Dirty Politics

The source

55. My next major project after the tax haven work was the book *Dirty Politics, How attack politics is poisoning New Zealand's political environment.* A copy of *Dirty Politics* is attached and marked as Exhibit "**NAH-2**". Dirty Politics was published by Craig Potton Publishing Limited. Copies of Dirty Politics went on sale to the public on 13 August 2014.

56. I began researching this subject, prior to receiving any leaked information. This was because I had been hearing stories about a dirty tricks team in the Prime Minister's Office that was coordinating attacks against the Government's political opponents, including with help from the political blogger Cameron Slater. I spoke to members of the parliamentary press gallery who suspected these activities but had been unable to prove them. They told me that when they asked questions on the subject, the allegations were always denied.

57. I was additionally interested in this subject because I was aware of the hundreds of personal attacks and smears on Cameron Slater's Whale Oil blog site and believed they were having a chilling effect on freedom of speech in New Zealand. Also, I had read the news reports about Cameron Slater's role in late 2013 in publishing very private details of an affair involving Auckland mayor Len Brown. New Zealand Herald investigations had shown that these revelations were part of an organised

NH
AAH 015

political attack linked to Len Brown's political opponents in the Auckland National Party. The campaign manager for the opposing mayoral candidate was Cameron Slater's father, a former president of the National Party. Considering these various signs together, I decided it was worth trying to research this subject.

58. I did not intend this to be my main work for the 2014 year, but rather something I would work on alongside other more advanced projects. This changed in or around March 2014 when I made contact with a person who claimed to have a quantity of information about Mr Slater's activities. Over a number of weeks we discussed the materials the source held, and I was given access to read them.

59. The source claimed to have come into possession of the information as a result of a "hack" of Mr Slater's computer. I was aware that this meant that the information was said to come from an unlawful source. I therefore carefully considered whether the public interest in the publication of the information was sufficient to justify its publication given these origins. I was of the view that this required a high level of public interest. After reviewing the material the source had, I formed the view that that test was met. I also considered that my use of the information would be preferable to what I knew to be the alternative.

60. Prior to me making contact, the source had been intending to disseminate the materials anonymously to the news media, using Twitter. The source's plan was to release them in a largely unsorted, bulk form. After I read the materials, I asked if I could use the politically important information, which represented a small fraction of the total, to try to produce a book of lasting value. I also argued that most of the material was private or unimportant and should not be made public. The source agreed to both parts of this.

61. All of my works are intended to disseminate their contents to the public; those contents being news and observations on the news. That is the whole purpose of being a journalist.

NKT
AAA. 016

62. Sometimes, as in the case of *Dirty Politics*, I use a book as the best medium for this purpose. A book is the better medium when I need to tell a large and complex story in sufficient detail to be understandable. A book allows me to be more detailed about the material I am relying on for each assertion of fact. A book is more durable. A book will be able to be referenced for years to come. It is therefore the better medium to use for stories that will have lasting importance.

63. I gave specific assurances to the source. I said we would put a "fence" around us, so that only the two of us would ever know about the source's involvement in providing the information. I said this assurance would last for the rest of our lives. I made these promises before I was shown any material. Indeed, I would not have been shown any material without making these commitments.

64. In keeping with my standard procedures, I never phoned or e-mailed the source, so that I would leave no electronic tracks between us. I never wrote down the source's name or any identifying information.

65. In order to persuade the source to share the materials with me, I had to explain my intended use of the materials. I told the source about my intention to write a book. The source was familiar with my past works, both books and articles, and would have understood that the material could also be used for articles.

66. After publication, I openly and repeatedly explained in interviews that I had based the book on material given to me by a confidential source.

Contents of the leak

67. I found many important stories in the materials provided by the source. These included a staff member in the prime minister's office, Jason Ede, going inside the Labour Party's computer systems during the 2011 election campaign and helping Cameron Slater choose information to use to discredit the Labour Party; and the Prime Minister's Office orchestrating the release of Security Intelligence Service information to Cameron Slater to

AAA · NH 017

use to attack the Labour Party leader during the same election. There were similar stories from the 2014 election, although the materials came from early in the election year so subsequent events were not so well documented.

68. There were many stories of abuse of government power, including misuse of the Official Information Act. There was evidence of unethical behaviour by ministers of the crown and by a senior member of the Police. The materials, for instance, showed the Minister of Justice providing the name of a Ministerial Services employee to Cameron Slater. She mistakenly believed this man had leaked information about her Government. The official was attacked viciously on the Whale oil blog site, leading to death threats being made against his family. Overall a pattern emerged of an underhand and manipulative style of politics, quite different to how those politicians were presenting themselves to the public.

69. Systems had been put in place in the Prime Minister's Office to avoid these activities being discoverable through the Official Information Act, parliamentary questioning, or other normal channels of government accountability. Jason Ede, the main person in the office involved in these tactics and liaising with Cameron Slater, had been shifted from his Ministerial Services salary to a National Party-paid salary in 2011/12, while his duties continued the same, meaning that he was no longer covered by the Official Information Act nor parliamentary questioning of his minister. This staff member conducted much of his business from non-parliamentary e-mail addresses so that they were inaccessible to the Official Information Act as well.

70. I continued research on the subjects in my book in early 2015, including using the Official Information Act to request information from the Office of the Prime Minister about communications between key figures in the book. I requested copies of all correspondence between Jason Ede and Cameron Slater and David Farrar from January 2008 until December 2011 - i.e. a period when he was paid by Ministerial Services - and the same

information for communications between four other staff in that office and Cameron Slater and David Farrar from 2011 to 2015. I also asked for copies of all correspondence between the Prime Minister's staff and Jason Ede from 2011 to 2015. The prime minister's chief of staff Wayne Eagleston replied on 11 March 2015 refusing to release any of this information, apart from a half a page of information previously released to the media by the Prime Minister. This illustrates the way that normal channels for obtaining government information do not work for the subjects I was exploring in the book.

71. Even when collaborating with the Prime Minister's Office, Slater was a private individual and not covered by freedom of information laws. As a result, there was no normal way to seek information about his activities either. This is precisely the sort of situation when information from leakers and whistle-blowers can be crucial for informing the public and parliament, and holding ministers accountable.

72. I had about twenty secondary confidential sources for the book as well. A National Party employee initially alerted me in 2012 to some of the issues that would later appear in the book and provided some documentary evidence. Several people shared their stories about being targets of Cameron Slater and his associates, on the basis that I would not identify them. After I got the leaked materials, I found and got help from several more confidential sources as I followed up and documented individual stories. In each case, these sources provided their information to me on the understanding that I intended to use it to produce books and articles intended to convey that information to the public.

73. In every case, I promised these confidential sources anonymity so that they would agree to share information with me for the purpose of that information contributing to a news story.

Response to the book

74. The book had the strongest public response within New Zealand of anything I have ever written. Many thousands of people attended talks I gave at universities, libraries and other public events during my August-September 2014 book tour. To date the book has sold over 20,000 copies, more than any of my other books.

75. As stated above, since the publication of *Dirty Politics*, I have had published two articles based on the same materials. I have also participate in many radio interviews, television interviews, and public speaking engagements, discussing the revelations contained in that book.

76. Also as stated above, I have been continuing my research into the matters addressed in *Dirty Politics*. It is intended that that new research will combine with the information in the book to be the subject of further works.

Further actions I took to protect my sources

77. In August 2014, I completed researching and writing the book and the publication date approached. I took the precaution of returning all copies of the leaked material to the source. I did this as a standard source-protection practice as in other projects. In fact, my source told me that all data that might point to the identity of that person had been removed before it was given to me and, to the extent of my technical knowledge, this appeared to be correct.

78. Some of the same data that had been provided to me was later leaked publically. This was done by the source using the pseudonym "Rawshark". I have looked at that publicly released material and it is identical to some of the material that had been provided to me. To the extent that that material was capable of identifying the source, I assume that this would already have been done by the Police.

79. This information release was in response to a challenge from the Prime Minister. I had given public interviews in which I had explained about my practice of removing the material from my possession. Shortly after that, seemingly in response to it, the Prime Minister publically accused me of making up the information in *Dirty Politics*. He challenged me to release the source material. I was asked in an interview what my response was. I said that I would ask the source to release some material to substantiate the information in the book. It was shortly after that that Rawshark started releasing materials.

80. Meanwhile, prior to publication, I then deleted all the leaked materials and related work off my computers, using a security programme that overwrites deleted space on the computer multiple times. Merely deleting a file does not remove its data from the computer storage and leaves it accessible to someone with sufficient technical expertise. By overwriting the data multiple times in a number of different ways, that possibility is eliminated.

81. Finally I collected and removed all notes and records used in the preparation of the book to ensure there was nothing left that could be traced to the source. As far as I am aware, I had been careful from the beginning of the project never to record anything that would identify the source. But, following my usual procedures, I took these precautions anyway. This was not because I expected a Police search. I did not. There had never been a Police search with earlier projects and books, even though in some of these cases there had been investigations into my sources.

82. By way of contrast, there was also a Police investigation after my publication of *The Hollow Men*. That investigation lasted for over a year. Near the end of that period, I was invited to attend the Wellington Central Police Station for an interview. I willingly participated in that interview. In the case of *Dirty Politics*, the first time the Police contacted me was on the phone while they were raiding my house and only because my daughter, who was present at the house at the time, had called me.

AAI · NH 021

83. In interviews following publication of the book, I was asked media questions about the source material, including whether I could provide it to other media and whether I was confident my source would remain confidential. I explained in these interviews that I had returned the materials to the source and that I had cleared out the house.

84. In addition, I questioned my main source in detail about precautions they had taken to ensure the materials could not be traced back to them. I was assured that all identifying marks and data had been thoroughly removed from the documents. I believe this person to be experienced and competent in the use of computers so these assurances were credible.

85. I am confident based on my own knowledge of source protection techniques, based on the steps that I took in relation to dealing with the main source for *Dirty Politics* both during and after my work on that book, and based on expert advice I have received from others including computer experts, that there was no material in my home at the time of the search that could assist anyone to identify the main source for *Dirty Politics*.

Relationships with confidential sources

86. During more than twenty years of this work, I have had many dozens of important confidential sources. In my experience they are very rarely reckless or disaffected people. They tend to be thoughtful, well informed people, who think carefully about what they are doing and who are motivated by public interest concerns. Some are in very senior positions, some in more junior positions.

87. We discuss the potential risks to them personally of providing information, including to their employment, families, and reputations. Some are very nervous, with conflicted feelings about wanting to blow the whistle on something they see as wrong, or too secret, but also fears about what might happen to them. Sometimes I have talked people out of giving information if I thought it was too risky to them or they were too uncomfortable.

NH

CAA 022

88. A number of times I have approached people who agreed to be sources in stories and they have subsequently told me that the reason they were willing to help is that they were aware of my approach in earlier books and projects and felt safe dealing with me. To date, I have never had a source identified, despite some concerted hunts to try to find them.

89. I have different types of sources. Some are not very sensitive, such as people I can phone off the record to check a story or some facts. Others are very confidential and without them many projects would be impossible.

90. When I am meeting a new source, I inquire in detail into their motives for helping me. As I wrote in some investigative reporting notes for a presentation to mid-level journalists at Fairfax, "If a source comes easily, or comes to you, you need to be suspicious. MOST sources are not our sources, they're using the journalist." I have a personal rule that I do not take stories from political people, or others with strong agendas of their own, as I do not want to be used for their purposes.

91. This applies to the book *Dirty Politics* as well. I have got to know the main source and I understand the person's motivations and circumstances well. As far as I am aware, the source is not politically active, is not a member of any political organisation, and is not closely associated with anyone who is. If there had been any suggestion that the leak had been politically motivated then, especially given the suggestion that the material may have been unlawfully obtained, I would not have had anything to do with it.

92. When writing critically about government and politics, it is common to be accused of being partisan and one-sided. But in my experience all governments are too secretive and at times abuse power. My body of work shows that I wrote the same sorts of stories and at times received the same sorts of attack-the-messenger reactions when I wrote about the 1999-2008 Labour-led government as I do under the current National-led government. For instance, the book *Seeds of Distrust* (known in the news as the "Corngate" issue), my reporting on the war on terror years, and the book

NH
AAA 023

Other People's Wars were primarily about government actions that occurred during the Labour government years.

My procedures for relating to sources

93. Since the late 1990s, I have regularly lectured to journalism students at various journalism schools. During these lectures I explain my personal procedures for trying to ensure the protection of my confidential sources.

94. My most regular lectures are at the Massey University journalism course, the Auckland University of Technology journalism course, and the Christchurch Broadcasting School. I have work experience students each year from the Massey University journalism course. I have also spoken to the journalism courses in Hamilton, Rotorua, Canterbury University, and Invercargill. I have helped run training courses for working journalists, for instance an annual training course for mid-level Fairfax reporters held in Wellington.

95. In July 2010, I helped conduct another Fairfax training day on investigative reporting. My typed notes for the day contain some of what I said to the journalists attending the event. Six of the eight pages of notes concerned sources and explained some of my ideas about source protection. "The first approach to a potential source is crucial," I wrote. "Protecting your source must begin right at the start, with no electronic tracks between you, no asking other people about the source etc. Subsequent meetings need to be treated with care too, or else by the time the publication date approaches you may have left too much evidence of your links behind to be safe.... We don't deserve people's trust unless we take this care." This sums up my actions in relation to the sources for the book *Dirty Politics*.

96. I am also invited to speak at overseas events, including being a keynote speaker at the first Global Investigative Journalism Conference in 2001 and being a speaker or on the organising committee of three subsequent Global Investigative Journalism Conferences. My recurrent theme, as in my speech notes for a presentation in Norway in 2008, was that "we have to be

utterly faithful to our sources". Similarly, I spoke at conferences in London and Sydney in December 2014 and, as one of the participants tweeted from the Sydney event, I argued that "if I give up my sources, why should anyone ever trust me again?" It should have been evident to anyone who looked at my work and public lectures that I was going to take a lot of care not to leave any evidence that would help to identify the main *Dirty Politics* source.

Immediate reaction from sources to the Police search

97. Following the 2 October 2014 Police search of my house, I had worried approaches from past and present confidential sources who were concerned that the raid might have compromised their confidentiality. In one case, it was a person with whom I am part way through an investigation about Police actions. This person knew I had files relating to this research in my house during the raid and was worried that these would have been seen.

98. Another approach was from a current source who was very worried about being identified. I met him twice to assure him that the Police did not appear to have found the notes of our previous meetings. The person repeatedly asked me whether I was sure that the person's identity had not been revealed and said they had lost a lot of sleep about the matter ever since hearing about the raid.

My approach to handing leaked materials

99. When I write a book or article there are many checks and processes that I follow to try to ensure that it is as fair and accurate as possible. In the case of *Dirty Politics*, I had access to thousands of Cameron Slater's and his associates' e-mails and other materials. I decided that nearly all of them were legitimately private or did not reach a standard of public interest that justified them ever being publicised. There was only a small proportion that revealed previously hidden collaboration with politicians and their staffs, and with industry lobbyists and PR people who were paying to have

AAA - 025

stories placed on the Whale Oil blog site attacking their opponents (notably, attacking public health professionals for their work on tobacco, alcohol, and obesity).

100. I felt that publishing this material was genuinely in the public interest. It disclosed important information about unethical activities, going up to the level of the Prime Minister and the Minister of Justice. It also revealed the background to other organised political attacks such as the revelations about Len Brown's affair.

101. Nonetheless, I still took steps to remove unnecessary documents and details from the text and removed the names of people only incidentally involved in the events and communications. In this way I was trying to use an important source of information but also to minimise the damage to other interests, especially personal privacy. I made other checks to ensure that the leaked materials were authentic and the facts within them were correct. In my experience if I make any mistakes at all, even one incorrect date out of a whole book, it is quickly pointed out by critics. In this case no one pointed out any errors of substance.

102. As mentioned, I had suggested the source not release any of the private and low-public-interest information that I was not using myself. On one occasion after release of my book the source made a mistake and released some information that had not had the personal parts removed. The source subsequently apologised publicly (still anonymously) for this and was more careful afterwards. I consider the source to be a thoughtful and responsible individual.

The search

103. I was called on the telephone by my daughter early on 2 October 2014. My daughter lives with me at 73 Grafton Road, Roseneath, Wellington. I was away at that time staying in Auckland.

104. My daughter told me that there were a number of Police officers at our house with a search warrant and that they had said that they intended to

search the house. She told me that she had tried to telephone my lawyer, Steven Price, but that she had been unable to get hold of him. I asked her to pass the phone to the Police officer in charge so that I could speak to him.

105. The phone was passed to someone who identified himself as Detective Sergeant Beal. He explained that he was searching for evidence of the identity of the main source of *Dirty Politics*. He read out some of the terms of the search warrant.

106. I told him that there was nothing in the house that would help them to identify my sources, but that there were many sensitive things related to other projects and confidential sources. I expressed concern that his search would interfere with my rights and obligations in relation to those other matters and confidential sources. He told me that he would make a phone call and get back to me.

107. I spoke to DS Beal again soon after that first call. I repeated my position that they would only find material related to other matters. DS Beal told me that they had to search the material to look, for example, for deleted files. He also told me that if they found information in material not related to *Dirty Politics* that was of interest in relation to other serious offending then they could act on it.

108. DS Beal then asked me whether I was claiming journalistic privilege in relation to the material in the house. I said yes. He then assured me that they would seal up all of the items they were seizing and not look at them without permission from a judge. I made it clear at that point that as far as I could tell from a distance everything that the Police might want to search was privileged. DS Beal accepted that and told me that everything would be treated as such. As I explain below, the Police went on to break this undertaking a number of times during the time that they were in my home and afterwards.

NH
027

109. At some point, either directly or through my lawyer, Steven Price, DS Beal informed me that I was not a suspect in the investigation of any offending at this point. I was told I was being treated as a witness. I remember being told that, and that that information came from DS Beal, but I cannot now remember exactly who told me.

110. I later spoke on the phone on a few occasions with my lawyers, Steven Price and Felix Geiringer. One issue raised by Mr Geiringer was whether I had any correspondence from lawyers on my computer systems containing legal advice, including correspondence that Mr Geiringer and Mr Price had sent to me. I did. I told them that there was such material on my computer. Mr Geiringer told me that he would communicate this to DS Beal. Later, Mr Geiringer told me that he had communicated this to DS Beal.

111. I was later told that my claim of privilege over everything meant that my daughter's property was also going to be seized, and for an uncertain amount of time. This was going to cause significant hardship to my daughter. After discussions, I waived any privilege that I might have had over anything on her smartphone. The Police also agreed to allow my daughter to remove some files from her laptop.

112. At no point did I authorise the Police to examine any of my material. Nor did I authorise the Police to use my internet connection.

113. Since soon after the raid by Police, I have been asking the Police to disclose to me, under the Official Information Act and Privacy Act, all of the information that they hold about the search. To date, very little information has been provided to be in reply to those requests. I know that those responses are incomplete because I have received more information through discovery in these proceedings. The existence of much of the material provided during discovery has not even been acknowledged during the OIA and PA processes meaning that I am not allowed to make use of it outside of these proceedings.

NK
AAA 028

114. The Police also resisted providing material to me via a discovery order. When I received those documents they showed that the Police had breached the undertakings given to me by DS Beal. Those documents also showed that the Police had been treating me as a suspect and had made a number of invasive investigations into my private life.

115. The documents provided under discovery showed that Detective Abbot found a piece of paper during the search which contained two email addresses and a password, and that DS Beal had then told ECL Officer Donovan to attempt to access both email accounts using the password.

116. One of those accounts was in my name and was an account I had used. The other, was an account used by a confidential informant. I had never accessed that second account and I do not know why anyone would think that I might have done so. Both accounts were set up specifically for the purpose of enabling the confidential informant to send confidential documents to me.

117. The confidential informant provided me with information on the basis that I promised to keep the confidential informant's identity a secret. The confidential informant knew that the information was intended to be used to write a news story. It was important to that confidential informant that I maintain the confidential informant's anonymity. That confidential informant had nothing whatsoever to do with *Dirty Politics*.

118. Luckily, both accounts had expired. If the Police had gained access to either account I believe that the information in the accounts could have identified the confidential informant, the nature of the information that the confidential informant had provided to me, and the fact that that person was a confidential informant.

119. I understand that the Police connected to my internet account to attempt to access these accounts. I did not give the Police authority to connect to my internet connection.

CAA NHA 029

120. I understand from the documents provided under discovery that Detective Abbot found another piece of paper during the search containing instructions provided to me on how to download information from an internet-based storage service using a TOR – a system that anonymises the identity of the person accessing that site. The instructions were assisting me to get access to information that was being provided to me by a confidential informant.

121. Again, this confidential informant provided me with information on the basis that I promised to keep the confidential informant's identity a secret. The confidential informant knew that the information was intended to be used to write a news story. It was very important to that confidential informant that I maintain the confidential informant's anonymity. That confidential informant had nothing whatsoever to do with *Dirty Politics*.

122. Detective Abbot handed the piece of paper to ECL Officer Donovan who photographed it and emailed the photograph to the National Cyber Crime Centre. The documents suggest that investigations were then undertaken by officers at the National Cyber Crime Centre in relation to the details on the piece of paper. ECL Officer Donovan records later being told that those investigations did not reveal anything of interest.

123. I do not know whether the investigation did not reveal anything because the Police had not been able to access those documents or whether they accessed the documents and realised that they were not of relevance to their investigation. If the Police succeeded in accessing those documents the documents would have provided them with information that could have identified the confidential informant and the fact that that person was a confidential informant.

124. I understand from the documents provided under discovery that during the search Detective Ferguson found a mobile phone and, separately, a SIM card in my bedroom drawers. Detective Teo took a note of the IMEI number of the phone and the SIM card number. The day after the search of my home, Detective Teo, with the approval of Detective Senior Sergeant

Gary Lendrum, made information requests to Vodafone New Zealand Limited seeking information in relation to the use of the mobile phone and the SIM card and to Two Degrees Mobile Limited seeking information in relation to the use of the phone.

125. The mobile phone and the SIM card had been exclusively used to contact a confidential informant. The confidential informant knew that the information was intended to be used to write a news story. It was very important to that confidential informant that I maintain the confidential informant's anonymity. That confidential informant had nothing whatsoever to do with *Dirty Politics*.

126. I understand from the documents provided under discovery that Detective Abbot found a printed copy of an email from a named person to me. That person had been publically accused of being Rawshark on Mr Slater's website, www.whaleoil.co.nz. That person had nothing whatsoever to do with *Dirty Politics*.

127. That document was seized by the Police and Detective Abbot discussed the content of that document with Detective Teo who, twenty days later, completed a job sheet wholly concerning that document which was put on the investigation team's database.

128. I understand from the documents provided under discover that while ECL Officer Donovan had access to my daughter's computer for the purpose of cloning it, he loaded the computer's internet connection details onto the screen and photographed the screen. He then connected ECL equipment to my internet connection using the information that he had obtained from examining the computer. He did not have my permission to connect to my internet connection.

129. These examples show how freely the Police were willing to breach their commitment not to look at any of the contents of the seized materials until a decision had been made by a judge. I did not know until after I received the discovery documents that this undertaking had already been breached.

130. Each of these breaches caused me significant alarm. As explained, I have commitments to many people to maintain their anonymity. I take these commitments very seriously. I am pursuing this action to fulfil those commitments. That the Police have already breached their undertakings and attempted to access the information they said they would not access without an order of the court, apparently in each case where they believed they had found useful leads during their search, is a cause of extreme concern.

Confidential sources caught in the search

131. I work from an office in my home. Like any other investigative journalist, my workspace includes computers, current research materials, contact lists, correspondence, diaries, very large quantities of files, phones, audio recorders, cameras and other tools of the trade.

132. Investigative journalism is a slow process. I have many ideas and projects at once that I am gradually working away on, often for years. Usually one or two projects are taking most of my effort, while many others are on the back burner or slowly advancing as time permits. This means that at any time, I have a considerable number of partly-progressed projects in my home. I could not practically do my work otherwise.

133. Even though I had cleared my house of the *Dirty Politics* materials prior to publication, the house had many other sensitive files and papers. As explained above, it is my practice to clear away all files related to a project just prior to publication if there is a serious risk that someone may want to expose the identity of a confidential informant on whose information the publication was based. However, I clearly cannot do that when I am still in the process of investigating a story. Necessarily, I have material in my house during an investigation that may identify confidential sources in relation to those investigations. I also may retain materials that have come from confidential informants where, while it is still important that I maintain those informants' anonymity, there is little prospect that anyone will expend significant effort to uncover their identity.

NH
AAA 032

134. To be clear, I had materials relating to a large number of partly-progressed and completed projects in my house at the time of the search. Those projects included some projects related to all of the subject areas identified above. The two computer systems that were seized contained at least some files in relation to each of the projects I have been working on. There was also a large amount of sensitive material contained in the other items seized by the Police. With the exceptions explained below, these were unrelated in any way to *Dirty Politics*. Files relating to many of my projects have been seized by the Police. In total, my computer systems and other electronic devices contained an enormous number of documents.

135. For instance, when the Police executed the warrant I was working on sensitive documents obtained from Edward Snowden that had been shared with me by The Intercept news organisation. In order to be able to do my work, I had copies of Snowden documents and files of background research around the house. I had signed a contract with The Intercept news organisation undertaking to keep all the material secret until the research was completed and until legal and other decisions on publication were made.

136. One of the USB storage devices seized by the Police during their search contained unredacted Snowden documents. There were also interview notes with other confidential sources who I had approached during research on the Snowden stories. The Police search was a serious breach of my confidentiality pledges to The Intercept and these people.

137. The Police seized or cloned a large number of digital storage devices. A survey of what they chose to take highlights what happens when the Police are allowed to perform a search in circumstances where they cannot readily differentiate between material that falls within the search and material that does not, and where confidential sources are inevitably jeopardised in the process.

138. First, the Police seized or cloned 16 USB storage devices. Eight were taken from my daughter's bedroom and unsurprisingly contained her essays,

SAA NH 033

photos, and TV programmes. But the other eight were mine and, while including nothing related to the book *Dirty Politics* or its sources, included various types of information from other confidential sources:

138.1. as stated above, one USB device had the Snowden documents;

138.2. two contained confidential tax haven data that my investigative team was given by a vulnerable source on the condition of strict confidentiality;

138.3. one had New Zealand intelligence documents from a confidential source, and from my knowledge of that person and that person's circumstances I expect that the mere knowledge that the Police had seized that material would traumatise that source;

138.4. one contained an audio file of a formal interview with someone in a sensitive job, a person who would be very distressed to know that it had fallen into Police hands; and

138.5. one contained information from confidential sources that I was holding as a safety copy (as explained below) for a journalist colleague who is aware that this material has been seized and who has told me that they are very unhappy about that.

139. The Police also seized my dictaphone, which contained a number of confidential interviews that had nothing to do with the book *Dirty Politics* or the source. I sometimes record interviews with less sensitive sources, albeit still in many cases confidential ones. The difference is that they are supplying information that I do not think will lead to a serious hunt for the source. The idea that I would have taped my *Dirty Politics* source is ridiculous. No remotely competent investigative journalist would tape an interview with a source of that nature.

140. The Police seized 104 compact disks, all several years old. Hardly anyone uses CDs anymore, so the Police should have been aware that the chances that the CDs related to a recent project were minimal. Many of the CDs

contained innocuous information such as documentary films or family photos. However, about ten of them contain very sensitive information given to me by a confidential source in 2003. Some of this information went into articles at that time and some I have used since then for other projects, including in *Dirty Politics*. To be clear, that source has nothing to do with the main source for *Dirty Politics* or the private communications of Mr Slater.

141. Although those CDs are twelve years old, I have an ongoing obligation to protect the identity of the person who gave me the information, and even the fact that I received that particular information. The information could be used to narrow down and/or identify who had given it to me. I feel very uncomfortable about it being in other hands.

142. It is generally true of all of the information described above, that it either reveals the identity of the confidential informant or it could be used to assist someone to determine that identity. This is obvious in relation to such things as taped interviews, but it is generally true of leaked material. The fact that that material was not public means that there are a limited number of people who could have leaked it. Some pieces of the leaked material are likely to be more revealing then others. Having access to all of the material that has been provided to me by confidential sources could be very good evidence of their identities.

143. Anyone who has the slightest understanding of what an investigative journalist does would know that I would have such materials in my work place.

144. The Police also seized 104 pages of paper files. My lawyer, Steven Price, photographed these papers before they were sealed and taken away so it was possible for me to review what the officers had seized. An analysis of what they took shows again what happens in a search like this one where the Police do not have a clear idea of what material they are looking for.

SAA NA 035

145. Various of the seized documents appeared irrelevant and in no way covered by the warrant. The Police also took a random selection of pieces of paper where I had written down phone messages and the names and contacts of people I had met. Pieces of paper with names and contacts included a friendly elderly couple I met on a plane, a family I met while tramping, a Norwegian journalist, two old friends I met at a funeral and more than 40 other people equally irrelevant to the Police investigation and scope of the warrant.

146. Approximately a quarter of the documents were copies of correspondence and papers sent to me by someone who had been attacked on Cameron Slater's blog. Another letter had been sent to me by a private investigator whose client had also been attacked on Cameron Slater's blog. In each case I had had no contact with the people concerned until after the publication of my book. There were also my speech notes, a draft press release, and a meeting poster from during my book tour, someone's blog post about the book and contact with a Guardian journalist about the book.

147. More important, this assortment of papers included the identities of six of my confidential sources from other projects that stretch back over about a decade. One had helped me with information relating to one of the stories in the book *Dirty Politics* but none had anything to do with the source the Police were seeking. For some of them, the mere fact that they had been in contact with me, were that to become known, could cause them considerable difficulties.

148. These confidential sources illustrate the collateral damage possible to journalistic sources when Police undertake a search like this one. There would be numerous similar cases of confidential sources being seen if the Police were permitted to search through my computers and electronic storage devices. As I described in relation to my past work, I make use of a large range of confidential sources for each of the works I produce. The electronic material seized by the Police covers a large number of different projects. This includes past projects where there were still plans or a

possibility of follow up work, current projects, and possible or planned future project. The total number of confidential informants caught up in the Police search is difficult to estimate but would likely be in the hundreds.

149. I am contacted by large numbers of people each year asking for assistance, by mail, email, and phone. This includes many people who approach me with stories or problems that they hope I will investigate and publicise. Some of these are very sensitive or personal. Some go on to become confidential sources in that they provide me with information for use in my publications on the basis that I keep their identity secret. Many notes of this sort and the people's contacts were in my house. Various of these were among the material seized by the Police during the search.

150. There are also a number of journalists and authors whom I help with their own confidential projects. I had various files in the house when it was searched by the Police containing these other people's work and contacts.

151. I am also sometimes asked by colleagues to keep copies of important and sensitive materials from their own journalistic projects. These are called safety copies. There were various examples of this in the house during the Police search and, as mentioned above, in at least one case this material was seized by the Police.

152. While I claimed privilege over everything the Police wanted to seize, I do not assert that all of the items seized was privileged. However, it was not, and remains not, possible for me to particularise the claim of privilege. I was not there and was not able to view and vet the items, and have not been able to view and vet them since. Including everything on all of the electronic and storage devices, the number of documents seized is enormous. I have hundreds of confidential informants. Without reference to my documents I cannot remember all of the details of all of my confidential informants, nor can I give a considered view as to whether a particular document might identify a confidential informant. In any case, it is difficult in practise to see how to particularise such documents in a way

that is not self-defeating. I cannot, for example, say that I am claiming journalistic source privilege over all emails from a specified person without revealing that that person is a confidential informant. Lastly, everything that falls within the warrant is necessarily something over which I would wish to claim privilege.

The impact of the search on me and my work

153. My lawyers have asked me to record the impact of the search on me personally. On a practical level, the search has considerably disrupted my work. The seizing of both my main computers, which contain research materials, address lists, email archives and other resources, has been a major inconvenience. Only some of the material was contained on a backup hard drive that was still accessible to me.

154. Also my paper files were scrambled during the search so that I often cannot locate materials. In addition, many weeks of work time have been lost while I replaced equipment, re-established computer files, and then took the actions needed to protect my sources through the current court action.

155. Personally, it has been an unpleasant and demeaning experience. The Police did not just search my office. They searched through my bedroom and personal belongings, and through those belonging to my daughter, including personal letters and papers. If I was a suspect in a murder case or serious drug case, it may have felt more understandable that they combed through our personal lives. But I am a writer and investigative journalist. I am serious about doing my work ethically and in the public interest.

156. The experience was also insulting. For instance, I willingly accepting a low income to avoid conflicts of interest and be free to do public interest work, so I felt extremely insulted that the Police claimed to my bank, apparently without the slightest grounds, that they were investigating me for "suspected criminal offending, namely fraud". This may also have an impact on how the bank treats me in future. My work is based on

NA 038

maintaining trusting relationships with a wide range of people and an obvious impression when the Police raid your home is that you have done something wrong.

157. There is a pattern in New Zealand politics of politicians attacking the messenger when they are caught out doing things they preferred would not become public. After *Dirty Politics* was published, I received a series of personal attacks from the Prime Minister John Key and others. By deciding to raid my house, the Police made this worse. The implication to some sections of the public was that there was something criminal about my legitimate occupation.

158. Also, I cannot help feeling that the Police have subjected me to more rapid and intrusive action than is normal. I naturally compare the actions against me to investigations of more serious crimes such as the "Roastbuster" rape complaints. In most media or political cases, the Police err on the side of not laying charges and certainly do not turn up unannounced to raid houses or offices. I cannot think of a single other case involving media where the Police have acted so intrusively. I do not understand why I appear to have been treated differently.

159. For instance, at the time of writing this affidavit, it is over seven months since the book *Dirty Politics* was published and the Police have apparently made little progress on investigating a Labour Party complaint about Cameron Slater and Jason Ede accessing its computer systems. There is no sign that either man has had his house raided, or even been interviewed. In contrast on September 22, the day after the election and only about three weeks after Mr Slater complained about my book, there was a Police directive to prepare to raid my home. A week and a half later the raid was conducted. I feel that I have received special treatment.

160. My strongest personal feelings were when I discovered that the Police had obtained all the bank account and credit card records from my bank. It is very unpleasant to know that people have trawled unsympathetically through each transaction describing the times, places and activities of my

AAA 039

life. An implication of this is that they thought they might find me involved in some dodgy financial dealings, maybe paying a source or being paid by someone for working on the book, which I find deeply insulting. Instead all they would have found is the personal details of my modest income. My book had, in part, been about people who were paid very well to do unethical and possible unlawful things, and here were the Police going after me, not them.

161. I was shocked that the Police felt it was appropriate to get my bank information without a warrant, through an informal arrangement with the bank industry lobby group, the New Zealand Bankers Association. The Police also sought personal information about me from Spark, Vodafone, TradeMe, and Air New Zealand, each time without going through the process of applying for a production order. The Police documents also include a directive instructing that a production order be prepared for my "telephone data and any other online data that can be captured" [redacted] but the documents do not record if these went ahead. I understand that the Police have a job to do but their approach to me and my rights feels cavalier as well as disproportionately intrusive. My impression is that the Police had made no effort to understand or respect the role played by someone like me in society.

162. The final, and most important, impact may yet be on my work. If the Police search is judged to be lawful and the Police are permitted to search my computers and other seized materials - a continuation of the fishing trip that began in my house - then everyone I ask to help me on sensitive projects from that date forward will wonder if the Police will arrive again and their confidentiality will be breached. I am certain this would impact seriously on my ability to do my work and to play my role effectively.

AA. NA 040

Return of my property

163. Since shortly after the raid, I have been seeking to arrange for the return of my property. When it was taken, it was on the understanding that I would be able to agree a procedure with the Police that would facilitate it being copied or cloned, with the originals being returned to me. About a week after the raid, my lawyers approached the Police with such a proposal. However, the Police have not been willing to agree to a process that is practical.

164. In December 2014, the Court determined that I could have my property back in accordance with a procedure proposed by the Police. However, this procedure required that the Police be allowed to do all of the copying themselves. I did not feel that I could submit to such a process unless I could have that process observed to ensure that it was not abused by the Police. At the time I considered that that was just the minimum precaution that my obligations, given the sensitivity of the documents, required. However, since that time I have discovered (through the documents reluctantly provided by the Police through discovery) that the Police had already breached a commitment not to examine the contents of any of the items seized.

165. I made enquiries that showed that paying to have the process proposed by the Police adequately supervised would have been prohibitively expensive. It would have cost more than an order of magnitude more than replacing all of the seized property with new equipment (albeit replacing the equipment would not result in my information being returned to me).

166. I have agreed to have two items belonging to my daughter cloned and returned without the cloning process being observed. This was because the information that might have been on those devices presented a low risk of revealing any information covered by journalistic privilege. Conversely, the hardship that was being caused by the deprivation of that property was greater and was being endured by my daughter. I therefore consented to the cloning of those items.

NA
CA 041

Conclusion

167. Thus my concerns about the Police search are fivefold. First, I have a professional obligation to protect the confidential source who provided me with information I used in the book *Dirty Politics*.

168. Secondly, I have an obligation to protect the confidentiality and privacy of all the other sources (and colleagues' sources) relating to whom notes, materials and contact details were in my house at the time of the search.

169. Thirdly, I cannot expect sources to help me in the future if they are not confident that I can hold information and work on stories without the Police arriving at my house and searching for the identity of sources. A general public perception that confidential sources are not secure, to which a Police search of my home obviously contributes, poses a serious practical risk to my work.

170. Fourthly, a high profile decision to legitimise the Police search of my house will also have a general effect, affecting the ability of other journalists to do their jobs.

171. Lastly, this search has had a direct and damaging effect on me and my work. It has caused me practical difficulties and interfered with my ability to do my work. It was greatly unsettling at the time and has since caused me great concern. It was, in short, a serious and, in my view, completely unwarranted, invasion on my private and work life.

Affirmed at Wellington)

on the 2nd day of April 2015) N. Hager

before me)

C. A. McLachlan

Barrister

C. A. McLachlan

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

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***

Affidavit of Bryce David Edwards

Affirmed: 31 March 2015

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

I, Bryce David Edwards, university lecturer of Dunedin, do solemnly and sincerely affirm:

Introduction

1. I have been asked to provide expert evidence to assist the Court on matters relevant to an application for judicial review brought by Nicolas Alfred Hager in relation to a warrant issued to the New Zealand Police to search Mr Hager's residence and examine his documents and computer systems.

Code of conduct

2. I have read the code of conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules. I agree to comply with it.

Background

3. As part of my academic work and my media work, I read *Dirty Politics* and I have been following the consequences of its publication. I am therefore very familiar with the background to this case.

Instructions

4. I have been instructed that it will be relevant to the Court's assessment of this case for the Court to understand the impact of the search of Mr Hager's property on the ability of the news media to access sources of facts and to communicate facts and opinion to the public in the public interest. As part of that assessment, I understand that the Court will want to consider the public interest inherent in the publication of *Dirty Politics*.

5. I have been asked to draw on the research that I have been conducting to set out what consequences there have been from the publication of *Dirty Politics* that are relevant to an assessment of its public interest. I have also been asked to draw on my expertise as a political scientist to give my own view as to the level of public interest inherent in *Dirty Politics*.

6. For the purposes of this assessment, I have been asked to interpret "public interest" to mean those matters that are likely to have an impact on the public or a significant section of the public, such that they are legitimately concerned about it.

My qualifications

7. I am a political scientist at the University of Otago, where I have been teaching and researching New Zealand politics since 2007. My scholarship on New Zealand politics relates mainly to political parties, public policy, and political communication. My recent research has focused on political scandals, digital politics (including the blogosphere), and the work of professional political party public relations experts (i.e. spin-doctors). The blogosphere is a term for the collection of blogs. A blog, short for web-log, is an online, self-published journal. It has become a common medium for the expression of political thoughts.

8. I have a PhD in Sociology from the University of Canterbury, which was on the history of political parties in New Zealand. I regularly participate in public debate about contemporary New Zealand politics via media interviews, and columns for various mainstream media outlets. These regularly include appearances on TV3 and TVNZ, interviews given on National Radio and Newstalk ZB and articles published in the New Zealand Herald.

Exhibits

9. Attached and marked respectively as "**BDE-1**" and "**BDE-2**" are two paginated volumes of exhibits to this affidavit. I refer below to documents within these bundles as **Exhibit [volume number]/[page number]**.

The revelations of *Dirty Politics*

10. Nicky Hager says in *Dirty Politics* that the book came about when he was leaked correspondence and other electronic documents relating to Cameron Slater. Mr Slater created and operates a blog known as Whale Oil Beef Hooked located at www.whaleoil.co.nz ("**Whale Oil**"). The Whale Oil site explains that the full name, Whale Oil Beef Hooked, is intended to be "said with an Irish accent". In other words, it is a play on "Well I'll be fucked".

11. Whale Oil is a mixture of news and commentary on politics and current events, and entertaining materials gathered from the internet. The commentary is generally right wing. Mr Slater's expressions of his opinions make extended use of invective and are frequently vitriolic. The site includes reader comments. These comments are said to be moderated, in other words that someone running the site vets their content and deletes them if they breach the site's rules. However, the reader comments are frequently extremely immoderate. They have in the past, for example, included people calling for the targets of Mr Slater's vitriol (and their families) to be shot.

12. The key revelations in *Dirty Politics* included that:

    12.1. senior members of the National government, including Cabinet ministers and people working in the Prime Minister's office, had been coordinating attacks on its political opponents with Mr Slater including by:

        12.1.1. providing Mr Slater with gossip to use to attack political opponents;

        12.1.2. assisting Mr Slater to publish material taken from the private parts of the Labour Party's computer system without authority;

12.1.3. assisting Mr Slater to make Official Information Act requests for documents that could be used to attack political opponents including information relating to the New Zealand Security Intelligence Service; and

12.1.4. delaying the release of documents damaging to the government to mainstream media journalists while expediting release of the same documents to Mr Slater so that he could put a pro-government spin on their content first and deprive the journalists of a scoop;

12.2. Public Relations agents had been drafting posts for Slater to publish for payment under his own name for the benefit of their clients, including posts attacking:

12.2.1. scientists and health professionals on behalf of companies producing unhealthy products such as sugary food and drinks or tobacco;

12.2.2. government policies on behalf of companies, eg tobacco and alcohol companies, who would be impacted by those policies;

12.2.3. the products of a client's competitors; and

12.2.4. unions in dispute with a client; and

12.3. a political advisor had been using Mr Slater to attack his clients' rivals for political offices, including:

12.3.1. a smear campaign against rivals within the National Party to Mark Mitchell's nomination as candidate for the safe National seat of Rodney before the 2011 election; and

12.3.2. what appears to be a plan to blackmail the then leader of the Act Party and sitting MP, Rodney Hide, into resigning

3C

to make way for Don Brash to assume leadership of that Party.

13. Many of the acts disclosed in the book are unlawful, some appear to be criminal, and some contradict previous public denials by senior politicians, including the Prime Minister.

Overall view of the public interest of *Dirty Politics*

14. In my view, the *Dirty Politics* book epitomises a publication that deals with crucial issues of public interest. The revelations of the book go to the heart of how politics work in New Zealand. They show how politicians attempt to influence public opinion and debate, and how this has occurred in a surreptitious way that seeks to mislead the recipients as to the source of the opinions. This information in Dirty Politics has helped the public to understand better how politicians work and the nature of political communication (particularly through the media and blogosphere).

15. In any democracy it is important that politicians – and especially Cabinet ministers – uphold the public's expectations of ethical behaviour. The Cabinet Manual states that ministers must operate with the "highest ethical standards". The revelations in *Dirty Politics* cast doubt on whether senior politicians were keeping to such standards.

16. In my view, *Dirty Politics* helps us understand how political tactics are used, and the relationship between media, politicians, and bloggers. The result of the publication of the book is that we have a better informed public debate and society.

17. In short, my view is that *Dirty Politics* is a work of significant public interest. Indeed, I regard it as a work of public importance.

18. There is no one scientific way of measuring public interest. However, in my view, we can examine a range of indicia to get a sense of the public interest in any particular matter:

18.1. the extent to which it is taken seriously by official agencies, the media, pundits, and academics;

18.2. the degree to which it engendered debate by the public and the media; and

18.3. whether the particular issues raised have current and ongoing significance to the wider public.

19. To explain how I reached my view on the public importance of *Dirty Politics*, I reflect below on how the book stands up to each of these possible measures.

An assessment of the accuracy and validity of *Dirty Politics*

20. The revelations and arguments made in *Dirty Politics* have been the subject of significant scrutiny since publication. By and large, the book has withstood that public evaluation. It is widely viewed to have been accurate in the facts that it presented and the analysis of those facts.

21. There has been very little that has been disproved in the book. I think this is remarkable. No academic study of politics ever gets everything right.

22. I am aware that Mr Hager acknowledges that he ascribed the wrong gender to a peripheral character in the book. I am not aware of any major or material claim that has been shown to have been false.

23. Any publication of this kind will be based on both research and the interpretation of that research. Mr Hager has done very well in his presentation of both. It is usually difficult to separate out facts from their interpretation. The presentation of *Dirty Politics* makes it easy for a reader to see where Mr Hager has presented the facts, and where he is analysing those.

24. That separation of fact and interpretation is important in terms of accuracy and validity. It means that Mr Hager is not presenting his opinions as facts. The material presented as fact is taken from Mr Hager's

3E Lab

source material, with that source material cited. It also means that the reader is able to understand the basis of Mr Hager's opinions and to test the validity of his conclusions for themselves.

25. What is particularly unique about Mr Hager's book is that it is based around the actual communications of the subjects of the book. In my view, these communications are presented in an appropriate manner. Overall, the level and quality of detail is impressive.

Responses to *Dirty Politics*

26. Below are some of the important responses to *Dirty Politics*. It is not intended to be a comprehensive list. It is intended to test the book against the measures identified above.

Official response

27. Some official inquiries were established as a result of *Dirty Politics*. The most important has been the inquiry by the Office of the Inspector-General of Intelligence and Security. This investigated whether the Security Intelligence Service ("**NZSIS**") had acted properly in the way that it disclosed information about a meeting between the Leader of the Opposition and the Director of the NZSIS.

28. A true copy of the final report of that inquiry is at **Exhibit 1/1**. The Inspector-General was highly critical of what had occurred in relation to the release of information. It found "significant failures by the SIS to meet its obligations". This investigation confirmed some of the revelations in *Dirty Politics*. It also vindicated the concerns Mr Hager expressed in *Dirty Politics* in relation to those revelations.

29. In an interview with John Campbell on 25 November 2014, Rebecca Kitteridge, the Director of the New Zealand Security Intelligence Service, acknowledged that the significant failures identified by that inquiry "came to light through [*Dirty Politics*]".

30. An investigation was also carried out by Justice Chisholm into allegations that Judith Collins had acted improperly in relation to the Head of the Serious Fraud Office. This did not relate to a revelation contained in *Dirty Politics*. Rather, it was a related matter that came about as a consequence of the media scrutiny into the matters set out in *Dirty Politics*, and also based on a piece of Mr Slater's correspondence.

31. A true copy of the final report of that investigation is at **Exhibit 1/81**. The report found that there was no evidence to support the allegations. The investigation did not encompass the allegations against Judith Collins that were set out in *Dirty Politics*.

32. The Privacy Commissioner is investigating alleged breaches of privacy by Judith Collins in relation to information she is said, in *Dirty Politics*, to have given to Mr Slater. I have also been provided with the Privacy Commissioner's determination in relation to a complaint made against Mr Hager for publishing Dirty Politics. The determination is significant in that it revisits the issue of whether a non-fiction book can fall within the news medium exception under the Privacy Act. A true copy of that determination is at **Exhibit 1/180.**

33. Other investigations have also been launched but have not yet been completed. The Police are looking into complaints from the Labour Party based on the revelation in *Dirty Politics* about the hacking of the Labour Party's computer system in 2011. The Chief Ombudsman has launched a wide-ranging investigation into the operation of the Official Information Act, which includes an investigation of criticisms contained in *Dirty Politics*.

34. This high number of official inquiries relating to one particular published book is quite extraordinary, and shows just how important the book has been. In addition it is worth noting that after the publication of *Dirty Politics*, three opposition parliamentary parties – Labour, the Greens, and New Zealand First – all called for a royal commission of inquiry into

issues arising out of the book. Such calls are not made carelessly. As stated below, this call for a royal commission has been supported by a leading academic.

Media response

35. *Dirty Politics* raised many questions about the role of the media in covering politics, and about the use by individual journalists of material from Cameron Slater. A significant debate has since occurred about this, with various journalists publishing their own accounts or explanations.

36. For example, New Zealand Herald investigative journalist David Fisher replied to the book with something of a mea culpa in the article, "My History with Cameron Slater". A true copy of that article is at **Exhibit 1/185**.

37. Elsewhere in the media there have been debates about the role of the media in the scandal. For example, TV3 News did a story entitled "Journos 'soul-searching' after latest Dirty Politics leaks". The video for that story is viewable at http://www.3news.co.nz/politics/journos-soul-searching-after-latest-dirty-politics-leaks-2014090210. A true copy of the text accompanying that video on TV3 News' website is at **Exhibit 1/189.**

38. A large part of my research involves following the coverage of New Zealand politics in the media. My strategy is to try to record and aggregate nearly everything that is produced on given topics. In the case of *Dirty Politics*, I have never witnessed such large amounts of media reportage and examination of one particular issue, let alone one particular book. Even measured against Mr Hager's previously controversial books, the media response was much more serious.

39. As a quick metric of media coverage, a search for the term "Dirty Politics" on the New Zealand Herald website, for 2014, brings up 532 stories. Similarly, a search on the Knowledge Basket database of media, brings up 27,887 documents for 2014.

Public response

40. The incredible public response to *Dirty Politics* is seen most clearly in the huge sales of the book – more than 20,000 copies were sold in 2014. In the first week of its release, *Dirty Politics* was the number one bestselling book in New Zealand, and according to the Nielsen Bookscan company, *Dirty Politics* was the fifth biggest selling book in the "New Zealand Non-Fiction for Adults" category for the 2014 year.

41. In addition, in the week after publication, Google's search engine rankings showed that *Dirty Politics* was New Zealand's most searched item online, while searches for information about John Key also doubled.

42. The relationship between the media and bloggers that is dealt with in *Dirty Politics* is clearly of great interest to the public. After the book came out, Horizon Research polled on the issue, finding: "More than half of adult New Zealanders (53.1%) believe mainstream media (newspapers, radio and television) have failed to act impartially in relation to material provided to them by bloggers". A true copy of the results of that poll is at **Exhibit 1/190**.

43. The same research found that "Large numbers of New Zealanders are aware of and talking about the issues raised as a result of the publication of Nicky Hager's book, Dirty Politics". It also suggested that there was significant public concern about the sorts of tactics outlined in *Dirty Politics*. Just over 80 per cent said they preferred it did not happen in New Zealand. The research report goes on to say that "The results indicate the Prime Minister, John Key, has made 135,700 people who voted National in 2011 feel angry, or disappointed or disgusted".

44. The public opinion research firm of UMR carries out on-going research into what political stories in the media are of greatest interest to the public. UMR's latest Mood of the Nation report, for 2015, shows that the controversies around the publication of the book, and then separately the

EE

resignation of Judith Collins (as a consequence of that debate) were two of the biggest political stories of the year, with 43% and 45% of respondents saying they followed these stories closely. A true copy of that research report of that poll is at **Exhibit 2/218**.

45. Another very interesting survey response was in terms of corporate CEOs. Business journalist Fran O'Sullivan reported in November 2014 that "The Herald's Mood of the Boardroom Election survey of CEOs found that 62 per cent felt "Brand Key" had been damaged by the Nicky Hager revelations, 66 per cent believed it exposed an unhealthy relationship between politicians and bloggers and 76 per cent of those surveyed raised issues of political probity concerning Judith Collins". A true copy of the New Zealand Herald article recording those results is at **Exhibit 2/280**.

46. In a time when the public's participation in politics is continuing to decline, there were surprisingly large numbers of people who attended public meetings where Nicky Hager appeared. Mr Hager gave talks all around the country. His Auckland meeting was attended, according to a TVNZ report by "around 400". A true copy of that report at **Exhibit 2/283**. Similarly, in Dunedin, Hager spoke to a public meeting (which I chaired) organised by a bookshop, which involved about 200 people paying $15 a ticket.

47. Much of the public also clearly felt, in 2014, that the revelations in *Dirty Politics* were such that they were taking them into account in terms of their voting decision for the general election. According to TVNZ, their in depth Vote Compass survey had 36% of respondents "saying the book has affected their voting decision". A true copy of that report is at **Exhibit 2/285**.

Academic response

48. Nicky Hager's books are not produced in a university context, yet academics appear to use his various books widely. I myself make particularly frequent use of his *Hollow Men* book in a number of courses I teach. In fact, it is worth noting that the foreword of that book is by academic Marilyn Waring, who makes this important comment about Mr Hager's methodology: "Nicky's approach is thorough. He generally assembles the subject matter in each 'case study' chronologically, so we can trace the emails, any other correspondence, the diary entries, and the newspaper coverage, point by point. In the social sciences we call this 'sophisticated rigour' and Nicky would mark very highly in this respect".

49. There will continue to be significant academic responses to the publication of *Dirty Politics*. I participated in a three-hour academic symposium entitled "Debating 'Dirty Politics': Media, Politics and Law", which has since been watched online about 4,500 times. A video of it can be viewed at https://www.youtube.com/watch?v=ZdgPh0Wh3g0.

50. Distinguished academic Dame Anne Salmond, the University of Auckland's Distinguished Professor of Māori Studies and Anthropology, has joined political calls for a royal commission. That view was accorded in a newspaper opinion piece entitled "Royal commission needed to clean up dirty politics", a true copy of which is at **Exhibit 2/287**.

High-profile people saying these revelations were important

51. A number of high-profile and important public figures commented upon the public importance of *Dirty Politics* in the weeks after it was released.

52. Leading political journalist John Armstrong (of the New Zealand Herald) compared the revelations to the most famous political scandal of American politics, pronouncing *Dirty Politics* as "The closest we've had to a NZ Watergate". A true copy of the New Zealand Herald article containing that comment is at **Exhibit 2/289**.

53. In another article, Mr Armstrong also explained that ""Hager's book goes to the heart of the Government". He commented on the reliability of the author saying, "no one has ever produced the evidence to question the veracity of the content of Hager's books. In short, Hager is credible". A true copy of the New Zealand Herald article containing those comments is at **Exhibit 2/296**.

54. The book's publication was also covered by the international media. For example, the *Guardian* newspaper ran numerous stories about it, including one feature by an Australian writer, Antony Loewenstein, who explained its importance, saying "It's extremely rare to have the genesis of a political smear campaign uncovered for all to see, just like it is uncommon to read the correspondence between senior government officials and media backers to attack opponents and critics. And yet, that is exactly what is unfolding in New Zealand. New Zealanders are currently witnesses to an exposé of unprecedented proportions." A true copy of the *Guardian* article containing that comment is at **Exhibit 2/299**.

55. Public interest in the book was asserted by many other high profile figures. For example, retired appellate judge Sir Ted Thomas spoke out about the book to one audience, as reported by David Fisher: "Sir Ted Thomas... told the crowd the author had an obligation as a journalist and citizen to make public information a hacker took from Slater's computer. He said the use of the information was outweighed by the public interest in having it revealed. He said it was "vital in a democracy deviant political practices are exposed". A true copy of the New Zealand Herald article containing the report of those comments is at **Exhibit 2/302**.

56. The "public interest" factor was also discussed in a newspaper opinion piece by Professor Simon Keller of the Philosophy school at Victoria University. He said "The role of political bloggers, as revealed in the book, is symptomatic of a larger trend toward the control and manipulation of information, not just by governments but by many

EE Lob

organisations that use public relations and communications consultants". He also noted that "a society in which such figures wield so much power is not a healthy democracy". His conclusion was that "Democracy, sadly, may depend on books like this one". A true copy of the Dominion Post article containing those comments is at **Exhibit 2/303.**

57. Probably the most surprising high profile public voice to give endorsement to *Dirty Politics*, was National Party member, lobbyist, and political commentator, Matthew Hooton. Despite being implicated in the book himself, Hooton wrote widely about the importance of the book and the issues it raised. For example in a political column in *Metro* magazine, Hooton discussed Mr Hager's credibility and declared that "nobody has ever shown his documentary evidence to be false". He argued that the operations revealed by Mr Hager amounted to "an appalling abuse of power", and that "After what has been revealed, the government deserves to lose on September 20 [the date of the general election]". In terms of some of those government operations, Hooton explained that "Parliament provides the Prime Minister with extraordinary powers" and that Hager's evidence showed they had been misused. In particular, he said that "the documentary evidence in Dirty Politics shows that Judith Collins, whom Key has entrusted with running the nation's police force, prison system, justice ministry, and accident insurance scheme, is not fit for senior office". A true copy of that *Metro* magazine article is at **Exhibit 2/305.**

58. Another senior conservative commentator, Karl du Fresne, also credited Mr Hager's investigation with great importance: "As irritating as Hager's sanctimony is, we are left with the disgusting reality that he has exposed government involvement in sleazy smear campaigns and machinations of a type that Richard Nixon would have approved. The political process, which has traditionally been remarkably clean in New Zealand, has been

EC Lab

tainted". A true copy of the *Nelson Mail* article containing those comments is at **Exhibit 2/309**.

Other consequences

59. At the centre of *Dirty Politics* are bloggers, disseminating political information and analysis online in the "new media". This area is one of great importance for electoral politics and public debate. The blogosphere has become a vital part of modern democracy and communication. But there are many problematic elements to it, which is why in recent years the Law Commission has been carrying out in depth research into issues relating to regulation and law of online activity. There has been much concern about "cleaning up" the blogosphere.

60. As a result of the publication of *Dirty Politics* there is now a definite move in the blogosphere towards greater transparency. Disclosure statements are more frequent. A number of bloggers have issued statements about their blogging policies. There is now greater clarity about the ethics of many bloggers. Some blogs have also now joined the Online Media Standards Authority, making them accountable to that body's code of ethics and a complaint procedure. For instance, leading blogger David Farrar has done so. He indicated that this decision was as a direct consequence of the *Dirty Politics* scandal.

61. As stated above, as well as affecting new media, *Dirty Politics* has had an impact on the interoperation of the traditional media with new media, especially in regard to how political party spin-doctors and bloggers are dealt with. This is an area in which *Dirty Politics* is likely to have its most enduring effects. For example, according to the news chief of TV3, Mark Jennings – the longest-running head of broadcast news in New Zealand – the impact has been considerable. He was reported as saying: "senior politicians have abused their power over information for political impact - and journalists have been caught up in politically-inspired 'black ops'."

EE Lab

62. Jennings is quite candid about what has happened: "Spin merchants are in all parts of society - politics, sports, fashion, you name it. We are never going to break the spin machine. But a powerful light has been shone on this and there will be some real introspection in the media".

63. Duncan Garner, who was previously the political editor for TV3, and continues to be a leading voice in political commentary, said: "From now journalists will be more aware of who they're dealing with". Clearly journalistic practices are changing as a result of *Dirty Politics*.

64. A true copy of the Radio New Zealand news report including these comments is at **Exhibit 2/311**.

65. As stated above, the political use of new media is a recent area of particular interest to me academically. In my opinion, *Dirty Politics* has had, and will continue to have, a significant positive effect in this area. Specifically, I believe that society will now be better able to read blogs and online social media. An enhanced scepticism towards claims made online is a very healthy outcome.

The important way that the *Dirty Politics* book was published

66. *Dirty Politics* has provided New Zealand society with a unique source of information about how politics works. The provision of that confidential information has been crucial for this, and there really is no other way that such information could have come out otherwise, and be properly understood.

67. Mr Hager has very usefully played an expert role as an intermediary with this information. I have no doubt that in checking, providing context, weeding out material that is not in the public interest or unreliable, and making the information accessible, Mr Hager has acted for the public good. He has carried out those functions extremely well. If the confidential information in *Dirty Politics* had simply leaked out – as some of it eventually did – the revelations would never have been properly

3E

analysed and contextualised. A simple dump or drip-feed would have been vastly inferior to having a journalist curate and analyse the material so that it could be properly comprehended.

68. Nicky Hager specialises in this methodology, and has come to receive an international reputation for the quality way in which he does this. Most of his media output is based on confidential sources, and provides a flow of important information to the public. He is to be commended for the public role that he plays.

Conclusion

69. Set out above, I recorded official responses to *Dirty Politics*, as well as responses from the media, the public, and academics. I have also noted public expressions of the importance of this work from high-profile commentators. I have considered the significant public interest of the contents of *Dirty Politics*, the clarity of its presentation, its accuracy, and the obvious care and skill with which it was produced. I have noted significant changes in the field of new media that have already directly resulted from its publication. I have recorded both my view and the views of others that *Dirty Politics* is likely to have an enduring effect in that area.

70. In my view, the conclusion that *Dirty Politics* is a work of public interest is inescapable. It has had a major effect on New Zealand politics and can be expected to continue to do so for quite some time.

71. Change may directly result from reports yet to be completed by the Ombudsman and the Privacy Commissioner. There may yet be a commission of inquiry into all of the matters raised in *Dirty Politics*. But whether or not that occurs, *Dirty Politics* has changed the way New Zealanders think about the political information they are receiving through both new and traditional media.

EE

72. This is why my conclusion is that *Dirty Politics* is not a just a work of public interest, it is a work of significant public importance.

Affirmed at Dunedin)
on the 31st day of March 2015)
before me)

L.E. Brown, JP
#13024
DUNEDIN
Justice of the Peace for New Zealand

~~A solicitor of the High Court of New Zealand~~ Justice of Peace . Linda Ellen Brown

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***

Affidavit of David James Fisher

Dated: 27 March 2015

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

I, David James Fisher, journalist of Auckland solemnly and sincerely affirm:

Introduction

1. I have been asked to provide expert evidence to assist the Court on matters relevant to an application for judicial review brought by Nicolas Alfred Hager in relation to a warrant issued to the New Zealand Police to search Mr Hager's residence and examine his documents and computer systems.

Code of conduct

2. I have read the code of conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules. I agree to comply with it.

Background

3. I have been reporting on this case and the underlying matters since *Dirty Politics* was published. I am therefore very familiar with the background.

Instructions

4. I have been instructed that it will be relevant to the Court's assessment of this case for the Court to understand the impact of the search of Mr Hager's property on:

   (a) the ability of the news media to access sources of facts and to communicate facts and opinion to the public in the public interest; and

   (b) the confidential informant(s) or any other person;

5. I have been asked to draw on my experience as a journalist who has made extensive use of confidential informants to give an opinion as to the likely impact.

6. I have also been asked to compare the events in this case to my experience of other requests by the New Zealand Police for information from journalists.

Experience

7. I have been a journalist for over 25 years. I regard what I do as investigative journalism. However, I would usually just use the term journalist to describe what I am. This is because I believe that all journalists should be doing investigative work as part of that job.

8. I have worked in New Zealand and in the United Kingdom. I am presently working for the NZ Herald where I have been for three years. Before that, I have worked in New Zealand for the Herald on Sunday, the Sunday Star Times, the Listener, and the Sunday News. In the United Kingdom, I worked for the Sun, the Daily Mail, and the Metro.

9. I have received a number of awards and award nominations for my work, the most prestigious of which were being named Reporter of the Year in 2007 and 2012 and being awarded the Wolfson Press Fellowship to Wolfson College, Cambridge University in 2007. At various stages, I have been named Business Reporter of the Year, Crime & Justice Reporter of the Year, Health & Education Reporter of the Year, and Government & Diplomacy Reporter of the Year, and I have been awarded a number of feature writing distinctions.

10. I have also guest lectured at AUT University, Auckland University, and the Journalism Training Organisation.

Police information requests

11. Unrelated to the remainder of my evidence, I have been asked to exhibit certain news stories I have written (two in 2012 and one in 2015) about requests for information made without warrant by the Police to banks and other private institutions. A true copy of these three news stories is attached and marked as Exhibit "**DJF-1**". Those stories accurately record the results of my investigations on this issue.

My use of confidential informants

12. I have made use of confidential informants throughout my career. In my present work, I would say that I use them on an almost daily basis. They are an integral part of my job.

13. Confidential informants have been an important part of my job since I started as a journalist. However, my use of confidential informants has increased during my career.

14. This is partly because the types of stories I worked on in my early career were of a less sensitive nature and did not depend so much on confidential informants. It is also because using confidential informants requires a great deal of skill. I have developed the necessary skills over the course of my career.

15. You need to know how to deal with people in a way that will put them at ease and enable them to trust you with their confidential information. You need to know who the people are: who will have access to information and what type of information they will hold. You also need to know what to do with the information once you obtain it. Lastly, you need to know how to protect the identity of the confidential informant and the sensitive information they provide. All of these skills require experience and maturity.

16. It can also be important to help confidential informants to be precise in what they provide. I have had circumstances where I had to dissuade people from providing too broad a category of information. It is possible, in some cases, to protect the source's anonymity, integrity and purpose by talking through types of information which exist to help refine exactly what it is they will leak.

17. Knowing what to do with information means being able to assess the public interest involved. Just because I receive confidential information does not mean that I will necessarily publish it.

18. For instance, it is essential to understand the motives of the person providing you with the information. It is possible that they are providing the information because they have an axe to grind or are seeking to rely on my story as ammunition for their private benefit. If that is the case then the information they provide is likely to be from a skewed perspective. In one example from my personal experience, the information was entirely misleading. In that case, proper investigation of the value of the information and the motivations of the source revealed the subterfuge and no story was published. Publishing stories not in the public interest is not what journalism is for.

19. It is also important to be able to distinguish between information that has public interest from information that is, for example, entirely prurient. The information I obtain from confidential informants is not for my benefit as an individual. It is for the people who read it. This places a responsibility on me as the recipient. I need to be able to judge whether information is genuinely in the public interest – in that it allows the readers to better operate in democratic society. Information that is not in the public interest is seen as such by the readers and is not welcomed by them.

20. Dealing with confidential informants can be a slow and gradual process. I remember one story where it was not until the confidential informant had been working with me for a year that they decided that they trusted me enough to give me their most important information.

21. Using confidential informants has therefore required me to spend a great deal of time getting to know them as people and getting to know their motivations and their concerns. As described below, a diverse range of people can become confidential informants. Nevertheless, based on my experience dealing with them I am confident of the accuracy of my views as set out below.

Nature of confidential informants

22. People leaking information with some personal ulterior motive are by far the minority. I have only encountered a small number of such people in my career.

23. In my experience, by far the majority of people who act as confidential informants have a genuine interest in seeing that the public are better informed. They are generally aware of current affairs. They have become privy to information which has been kept from the public and they know that the absence of the information leaves an important gap in public discourse.

24. I have dealt with confidential informants from all walks of life. Many are public officials, but they could just be neighbours who have come across some important information. Often they do not understand the full importance of the information they hold, but know that it is important and that it is something that has not been revealed to the public.

25. The promise of confidentiality is, of course, very important to them. I do not just promise confidentiality on a whim. They are confidential informants rather than just informants because it is very important to them that they are able to maintain their anonymity.

26. It is also relevant that promises of confidentiality are qualified. There is legal precedent abroad to waive confidentiality when it becomes apparent it is being used as a shield behind which to attack or deceive with malice. It has become my practice in recent years to specifically voice that qualification to people who I am approaching – or who approach me – as sources.

27. In my experience, confidential sources are very conscious of the jeopardy they are in. They expressly consider what might happen to them if they are exposed as a source.

Consequences of exposure

28. There are far ranging consequences should they be exposed. Obviously, in providing the information they are breaching some form of confidentiality obligations. It is possible that that may be enforced with criminal sanction. It is certainly common that breaching that obligation will be a breach of the confidential informant's employment obligations. The obvious consequences may include some form of criminal, civil, or employment process.

29. However, the consequences go much further than that. Confidential informants experience enormous stress. Both regarding the impact for themselves and, particularly, for their families.

30. It may be that they have only passed on a very narrow piece of information, and that they had very good reason for leaking that information. However, if exposed they risk being regarded as generally untrustworthy or generally unprofessional. Whether or not it is justified, they risk ruining their careers.

31. They also risk public attack and condemnation from people who have political reasons for not liking the leak. One can see that already with Mr Hager in this case. In my view, there can be no question that the material that was exposed in *Dirty Politics* was of the highest level of legitimate public interest. Nevertheless, Mr Hager has been subjected to a large number of nasty attacks on his character from a number of journalists and politicians, up to, and including, the Prime Minister.

32. Rawshark, if exposed, could justifiably fear similar treatment for himself and his family.

Likelihood of confidential informants being aware of this case

33. Based on my experience dealing with confidential informants and getting to know them over the years, I regard it as entirely inevitable that this case is going to have a significant effect on potential confidential informants.

34. There has been a great deal of public attention on this case and the events that preceded it. As stated above, *Dirty Politics* exposed a number of issues of the utmost public importance. Justifiably, a large number of stories in the media have followed on from those revelations. There has also been a significant media focus on Mr Hager and on Rawshark. The search was headline news across the country, and there continues to be significant media interest on the development of these proceedings.

35. I must acknowledge that I have covered these events myself. It could be seen that I am giving evidence of media interest to which I am myself contributing. However, I have been covering these issues because of the significant public interest in them.

36. I regard it as very highly likely that potential confidential informants will be conscious to some degree of the events in these proceedings.

37. The public consciousness of this story has been particularly high in Wellington. That is where Mr Hager lives, it is where the search happened, it is where the book was launched, and it is where these proceedings are taking place.

38. Wellington is also where most of my confidential informants are from. This is because a great deal of the confidential information of public interest comes from the various arms of government. A large part of the administration of the New Zealand government is seated in Wellington, and it is the hub of New Zealand politics.

39. As I said above, the confidential informants I deal with are very conscious of the jeopardy they are in, and they think through what might happen to them if they are exposed. Mr Hager is a high profile investigative journalist. The idea that the Police can come unannounced and seize essentially all of such a person's documents would be regarded by the confidential informants I have dealt with as a nightmare scenario. I am therefore in no doubt whatsoever that:

39.1. the result of this case will have a significant bearing on the decision making of potential future confidential informants;

39.2. if the Police are allowed to go ahead with this search, it will have a very significant chilling effect on the ability of Mr Hager and other journalists such as myself to receive information from such people; and

39.3. the corollary is also true that if the Police are not allowed to go ahead with this search, confidential informants will take comfort in their ability to speak with journalists.

40. To be clear, in relation to the second conclusion, it is my view that if the search is found to be legal, and the Police are allowed to review Mr Hager's documents, then as a result of that decision people who would otherwise have been confidential informants for the news media will decide not to do so due to the added risk that their identity will be exposed through a similar search.

41. The effect on Mr Hager himself is likely to be particularly pronounced. By that I mean that future potential confidential informants of Mr Hager's will be particularly affected by the decision of this Court in relation to this search. It will be even more likely that those potential sources will decide against sharing information with Mr Hager if this search is permitted to go ahead.

Noticeable change since the search

42. Since early October 2014, when it was reported that the Police had raided Mr Hager's home and seized his computer systems and other material, I have already noticed some change in the attitude of the confidential informants I have been dealing with. Since that time, I have noticed potential confidential informants are concerned about the possibility of having their identities exposed.

43. This is entirely anecdotal. The people I have been dealing with are not the same people I have dealt with before, so I am not comparing like with like.

070

44. I have also not raised the issue of this case with these potential confidential informants. While risks are discussed with potential informants, discussing the potential ramifications of this case is not likely to put them at ease about sharing their information. I therefore cannot say to what degree these people have been affected by this case.

45. I therefore have not relied on this observation to any significant extent in determining my views as set out above. I merely note it, as the observation is consistent with those views.

What will happen if confidential informants do not come to the media

46. If a potential confidential informant does not come to the news media then there are logically three possibilities. The most obvious possibilities are that they may decide not to leak the information at all, or they may try to do so through another means such as simply self-publishing by dumping the whole of the information in the public domain directly or through sites like WikiLeaks.

Anonymous leaks

47. The third possibility is that a greater fear of exposure created by this case would also lead to an increase in anonymous leaks to journalists, which is something that occurs from time to time. An example of this would be were documents are posted to me without any information about the sender. It is a type of leak which stands in a class of its own, in that it exists in a vacuum of credibility.

48. Every aspect of the leak must be proved while effort is taken to also protect the source, who may be inadvertently exposed. It requires giving as little away as possible in the proving of it, while being unaware as to the motives behind it. In some cases, anonymous leaks are unable to be used due to the difficulties that the anonymity creates in investigating the information.

49. As an example, I have been recently provided a computer file of a document. I do not know who sent it to me. When I try and open it, it checks with the

server of the originating public body and requires password authorisation. I have sought the document through the Official Information Act only to be told by the agency that the document does not exist. I can access file documentation which shows clearly it has come from the public body's computer servers and it identifies the name and time of the last person to edit it – a public servant who works at the body. It is now very difficult for me to progress any investigation, not knowing whether my inquiries will reveal the identity of the person who sent it to me. To prove the document exists, I would have to provide the document which could expose the source.

50. An increase in this type of leak does little for anybody involved, neither the reporter leaked to nor the organisation leaked from, given the possibility of people running material which has not been properly verified. It certainly does nothing for the source, who faces frustration over genuine material not being used and a higher risk of being accidentally exposed.

Online dumps

51. Having dealt with many confidential informants over the years, my firm view is that there are some people who would fall into each of the possible camps identified above. Some people are determined to release the information by whatever means. If they felt that it was not safe for them to do so through me then they could well decide to simply dump the information online. There are other people who I firmly believe, from my experience of getting to know them, would not take such a course. As discussed above, relationships have a lot to do with leaks. Working with a person to find out exactly what information they hold and to persuade them that they should provide that information can take a long time. I would not expect such a person to take it upon themselves to publically dump that material.

52. In my view, both alternatives are detrimental to the public interest.

53. As described above, there is a lot of work involved in making use of confidential information. It is not simply a matter of publishing the material

that is provided. The material is carefully vetted for public interest. Documents could well contain information that should be disclosed in the public interest alongside material for which there is a genuine reason why it is in the public interest why the material should not be publicly released.

54. The caution that the news media exercise is based on a great deal of experience dealing with matters of this sort. The process involves skill and experience to distinguish between what is in the public interest and what is not. I am able to call on colleagues including experienced editors in my newsroom to assist me with that process. It also can take a lot of work. Large numbers of documents may need to be sifted through or redacted. That may be something that a newspaper has the experience and resources to do, but a confidential informant does not.

55. There are plenty of examples of how dumping material can go wrong. In the case of Wikileaks, Julian Assange had a relationship with the Guardian newspaper. The newspaper had a lot of strict controls over what could be made public. Mr Assange fell out with the newspaper and decided to dump a large amount of unedited material into the public domain. That was damaging to a lot of people in a way that could not be justified in the public interest.

56. We saw the same thing with Rawshark. He put out an unregulated dump of Cameron Slater's conversation with Aaron Bhatnagar. That conversation included personal information which should not have been published in the public interest – for example, personal medical information about Mr Slater's family and sexual allegations against members of Parliament. That material would never have been published if it had been vetted by the NZ Herald and was not published in *Dirty Politics*.

Importance of confidential informants

57. The other possibility is that the potential confidential informant will not release the information.

58. It is extremely important in the public interest that confidential informants are able to provide material to the news media. The information they provide is simply essential to be able to produce the stories we produce. It is in the public interest that those stories are produced. As I say above, I wouldn't produce the stories I do based on confidential information unless it was in the public interest to do so. The extent of that public interest can be very high indeed. It is probably easiest to explain this with reference to a recent example.

59. In 2012, I reported on the 2010 Anzac Day crash of a Royal New Zealand Air Force helicopter in which three men lost their lives and one other was critically wounded. Following the initial reportage, I was given a copy of the Aircraft Accident Investigator's report by a confidential source. The document was the foundation document for the military Court of Inquiry report but was not publicly accessible, as it was a statutorily protected military process. Documents within the process cannot be obtained through the Official Information Act.

60. The copy of the report which was provided was written by the most experienced crash investigator in the Royal New Zealand Air Force and covered issues far broader than the accident itself. The breadth of vision and inquiry in the report was not conveyed in the final Court of Inquiry report.

61. The reason for this became clear on reading it. The Aircraft Accident Investigator's report identified systemic faults in the RNZAF which were contributing factors to the ANZAC Day crash. It identified faults in squadrons across the country and revealed the RNZAF's terrible record in enacting recommendations made through the Court of Inquiry process. In the case of the ANZAC Day crash, appropriate follow up of recommendations – which carried the force of an order from the Chief of the RNZAF - were factors in the 2010 accident which killed three men. Further, it pointed to specific incidents which had resulted from the failure to enact recommendations.

62. Among the specific incidents was the discovery that RNZAF had illegally transported a chemical pyrotechnic canister on an international Air New Zealand passenger flight to Canada, endangering the lives of all on board including up to 379 passengers. RNZAF had never reported the incident to Air New Zealand or the Civil Aviation Authority even though senior officers at the time warned, "it is important the RNZAF does not cover up" the incident. The quote is from a RNZAF document written in the wake of the incident.

63. The official public report from the Court of Inquiry gave a very different impression then the leaked report. It had sought to put the blame for the ANZAC Day crash on problems within the squadron, not broader problems affecting the whole of RNZAF. There had been no disclosure of other issues, such as the illegal transportation of explosives. I contacted Air New Zealand as part of my investigations and it had no knowledge that any such thing had taken place. The Civil Aviation Authority, which should have also been informed, had also not been told of the incident.

64. The leak of the report, and the publication of my story based on that report, led to an inquiry by the Civil Aviation Authority. More importantly, it became part of a major review of RNZAF procedures. The ANZAC Day crash investigations, in total, led to a number of inquiries which confirmed gaps in the safety systems and forced change which – while accepting the dangers inherent in military flying – make it a safer environment in which to operate. It seems very likely that the leak of that report has saved lives.

65. The individual who provided the Aircraft Accident Investigator's report to me was a genuine, well-meaning individual who loved RNZAF and respected the chain of command. The person was also deeply troubled that the streamlined Court of Inquiry report, which focused narrowly on the issues in one squadron, meant the expert investigator's findings would be overlooked. The person had good grounds to be concerned. The investigator's report recorded a number of previous internal reviews which

had been ignored, to the detriment of others and particularly those in the aircraft which crashed on Anzac Day in 2010.

66. The individual who provided the information feared that should their identity be known they could face court martial as well as isolation from their peer group and condemnation from commanders. The person had a genuine, and well-founded, fear of vilification.

67. In my view, the individual did New Zealand an extraordinary service by trusting me to do the right thing with the material which was provided.

68. Having gotten to know this person in the course of working on this story, I feel that they would not have been the type of person who would have self-published the material online. The person was aware of the line of inquiry I was pursuing and believed the report contained answers to the questions I was asking. In short, they trusted me to make appropriate judgments in relation to the material. Further, the report contained personal, medical information about an individual which would have had an extreme negative impact on that individual particularly and that person's family were it to be made public. The source trusted I would not use this information.

69. This story, and others I encounter, would not be possible to tell without the assistance of confidential sources. For me personally, stories of this sort with the impact this had and the changes forced as a result, do not come along with great regularity. It would have been impossible to tell this story, and others, without promising the person that no one would ever know who they were or that the information came from them. Such an assurance is critical to creating an environment in which a potential source has the freedom to do the right thing.

Previous experience of Police searches

70. I have previously experienced a number of instances where the Police have sought information from the news organisations at which I was working. In some cases, the information that was sort was information that I held. In

other cases, it was someone else in the organisation, but I was sufficiently closely involved that I directly witnessed the process employed by the Police.

71. My experience of these previous searches stands in stark contrast to the present case. One example is the events at the time of the 2011 general elections, involving what has become known as the Tea Pot Tapes. In that case, the Police were seeking information that the newspaper for which I worked, the Herald on Sunday, held. A member of the Police telephoned the newspaper. He spoke to the Editor. He told him that they had a warrant and explained what information they were seeking. They gave the newspaper time to prepare the information that was sought, to consider whether there was any information that should be withheld on the grounds of privilege, and, if necessary, to seek the review of the Courts. Members of the Police then attended the offices of the newspaper. They were handed the information they were seeking under the warrant. They left. There was no general search of the newspaper's offices. Nothing was seized beyond the requested item.

72. In all my dealings with the members of the Police, they have acted in a manner that suggested that they were conscious of the sensitivity of dealing with journalists who may have obtained their information from confidential informants and who may have claims of privilege over the information sought. That said, I have never before heard of Police seeking to execute a search warrant aimed at obtaining the identity of a confidential informant. Nor have I ever heard of the Police seeking to search a journalist's home or emails.

73. The approach described above is the one that has been followed in every Police search in which I have been involved. The most recent such example occurred in 2014 since the introduction of the Search and Surveillance Act 2012.

Campbell

74. I am familiar with the facts of the 2009 case of *The Police v Campbell*. I have been asked whether my views set out above would have been the same in relation to the facts of that case. They would not be the same.

75. The facts of the *Campbell* case are very different from the present case. I do not think that the level of public interest that exists in relation to *Dirty Politics* can be said to have existed in the *Campbell* case. It might have been interesting viewing but I doubt sincerely the viewers of the Campbell current affairs show would feel the host, as their proxy, had properly used his assurance of confidentiality in that case.

76. In the *Campbell* case, the criminal offending of the confidential source was the story. There was no matter of public interest that had been disclosed by the confidential source, albeit acting unlawfully in doing so. As well as diminishing the legitimate public interest of that case it also means that a person who is considering providing information to a journalist about the wrongdoing of others is unlikely to consider themselves to be at risk because of the *Campbell* decision.

77. The *Campbell* case also did not involve the execution of a search warrant on the home of a journalist or an attempt by the Police to conduct a search of all of a journalist's correspondence.

78. In my view, the decision in the *Campbell* case would not be expected to have had the sort of chilling effect that it is my view will result in this case if the Police are allowed to search Mr Hager's correspondence.

Nicky Hager

79. It is also relevant to my opinions above to consider the nature of the target of this search, Nicky Hager. Mr Hager is known in the journalism industry as firstly, a fine journalist, and secondly, as someone who is a master at developing and protecting sources. Mr Hager's reputation for source protection is of the highest order.

Conclusion

80. Based on my many years of work with confidential sources and on my knowledge of the facts of this case, I am of the view that if the Police are permitted to go ahead with their search of Mr Hager's documents then this will have a significant chilling effect on the news media's ability to access information. I believe that people who would otherwise have been confidential informants for the news media will decide not to do so due to the added risk that their identity will be exposed through a similar search.

81. Some people may instead self-publish information online. Others may attempt to leave information anonymously with journalists. I firmly believe that some others will simply chose not to provide the information they have at all. All of these alternatives are detrimental to the interests of society.

Affirmed at Auckland)
on the 27th day of March 2015)
before me)

I Esekielu

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

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***

Affidavit of Seymour Myron Hersh

Affirmed: March 2015

My Commission Expires
August 31, 2019
Leslie P. Kim
1718 M St. NW
Washington, DC 20036

SUBSCRIBE AND SWORN TO BEFORE ME
THIS 26 DAY OF March, 2015
BY Seymour Myron Hersh
NOTARY PUBLIC

LESLIE P. KIM NOTARY PUBLIC DISTRICT OF COLUMBIA EXP. 8-31-2019

Solicitor
Thomas Bennion
Bennion Law
L1, 181 Cuba Street
PO Box 25 433
Wellington 6146
Tel: +64 4 473 5755
Fax: +64 4 381 3276
tom@bennion.co.nz

Counsel
Julian Miles QC
Richmond Chambers
L5, General Buildings
33 Shortland Street
PO Box 1008
Auckland 1140
Tel: + 64 9 600 5504
miles@richmondchambers.co.nz

Felix Geiringer
Terrace Chambers
No. 1 The Terrace
PO Box 10 201
Wellington 6143
Tel: +64 4 909 7297
Fax: +64 4 909 7298
felix.geiringer@terracechambers.co.nz

I, Seymour Myron Hersh, investigative journalist of Washington DC, United States of America, solemnly and sincerely affirm:

Introduction

1. I have been asked to provide this affidavit to assist the Court on matters relevant to an application for judicial review brought by Nicolas Alfred Hager in relation to a warrant issued to the New Zealand Police to search Mr Hager's residence and examine his documents and computer systems.

Background

2. I am familiar with the general background to this case. As discussed further below, I know Mr Hager and am familiar with his work. I am aware that in August 2014 Mr Hager published a book entitled "Dirty Politics", and I am aware of the nature of the contents of that book.

3. I understand that Mr Hager says he based the contents of that book on material given to him by a confidential informant who has been using the alias Rawshark. I know that it is alleged that Rawshark procured that material by accessing a computer system without authorisation, which is a criminal act in New Zealand. I understand that the Police are investigating that alleged crime and that that is the purpose of the warrant.

4. Lastly, I am aware that Mr Hager is challenging the legality of the search of his premises and seizure of his property in these proceedings, chiefly on the ground that the processes leading up to it failed to take account of the public interest in him being able to protect the identity of his confidential sources.

Code of conduct

5. I have read the code of conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules. I agree to comply with it.

Instructions

6. I have been instructed that it will be relevant to the Court's assessment of this case for the Court to understand the impact of the search of Mr Hager's property on:

   (a) the ability of the news media to access sources of facts and to communicate facts and opinion to the public in the public interest; and

   (b) the confidential informant(s) or any other person;

7. I have been asked to draw on my experience as an investigative journalist who has made extensive use of confidential informants to give an opinion as to the likely impact.

8. I also understand that Mr Hager's credentials as a journalist may be relevant and I have been asked to comment on my assessment of Mr Hager and his work.

Qualifications as an expert

9. I have been an investigative journalist for over 50 years. My articles have appeared in a large number of prestigious publications. I have been a regular contributor to the New Yorker for the last 22 years. I have also published 8 non-fiction books and am working on my 9th. A large part of my career has involved investigations into military and security matters.

10. I have received more than 20 major prizes for my work including the 1970 Pulitzer Prize for International Reporting for my disclosure of the Vietnam War tragedy at the hamlet of My Lai. I have been awarded a George Polk Award for Journalism on record five occasions (1970, 1973, 1974, 1981, and 2004).

11. I have made regular use of confidential informants throughout my career.

12. I note that my experience is chiefly limited to journalism in the United States of America. In order to express the opinions set out below, I have had to assume that these experiences are transferable to the New Zealand context. I do not claim any significant knowledge of New Zealand. I am not aware of any reason why my views would not be equally applicable in New Zealand, but to the extent that there are material differences of which I am unaware these would need to be taken into account in assessing the relevance of my views.

Public importance of confidential informants

13. The use of confidential informants has been essential for my work. I could not have produced the stories I have without their assistance.

14. The information I have been able to impart to the public through the use of confidential informants has included matters of major public importance. The first and most famous example is the information I was able to expose over the massacres at My Lai.

15. That article needs to be understood in its context. There was extreme censorship during World War II. The American public had very little idea what war was like. The My Lai story put pay to the notion that American soldiers were brave pilots flying with no headgear, their canopies open, wearing a white scarf, and giving a thumbs up sign as they flew off to fight a noble fight. It showed the ugly reality of war and that our good, decent boys could behave as beastly as the hated enemies of World War II.

16. That story would not have been possible were it not for people in the United States military who were willing to share with me the proceedings of the Army's own secret investigations as they took place.

17. That is just one particularly well known example. It illustrates both the vital part that confidential informants play in exposing stories, and the enormous benefit to the public that such stories are exposed.

18. The sad, but inevitably true, fact is that claims of national or state security are, in the overwhelming majority of cases, done for political purposes. In my experience, claims of national security cannot be taken at face value. They need to be evaluated. Far more often than not, they are not justified. It is therefore necessary for there to be people willing to breach those claims of confidentiality.

19. By claiming confidentiality, State agents are able to avoid scrutiny. Unjustified claims of confidentiality are therefore easily used to hide wrongful acts by the State. In far too many case, they are used to protect the State from criticism or embarrassment, rather than furthering the legitimate interests of the public. Without people willing to give material deemed confidential, to the news media, it would not be possible for unjustified claims of confidentiality to be challenged.

20. That is not to say that I necessarily reveal all confidential information that is provided to me. I have withheld stories because I, my editor, my publishers, and, very often, senior military and intelligence officers in whom I had trust, had concerns that there were legitimate reasons for withholding the relevant information. It is my experience that competent news media can be relied on to access material and to publish only where there is a public interest in exposing the information that outweighs any reasons for confidentiality. Indeed, they are, in general, far more reliable in that regard than the agents of the State.

Nature of confidential informants

21. I never use information from a confidential informant unless I know who the confidential informant is. I am not interested in being used as a pawn in a political battle or as a means of revenge for some disaffected person. It is therefore important that I know and understand the sources of the information and their motivation for providing it to me.

22. It is also important for my editors and publishers. They may not be able to confirm that everything a source says is true, but they will want to at least verify that the person giving me the information is a person who is in a position to know that information. The New Yorker is particularly well regarded for such fact checking.

23. In my experience, in the field in which I work, confidential informants are intelligent thoughtful people. They are serious people with a legitimate complaint that deserves to be shared with the public. They are people who are engaged with society. They include senior public officials of all kinds. They have access to the information they are providing through their roles and are frequently still involved in those roles. They are often people who intended to make a positive contribution to society through their work but who are for some reason, usually political, being prevented from doing so.

24. Going public, and losing their jobs, or facing criminal prosecution, is not an option for most informants, who view truth as vital to democracy. It is not reasonable to expect everyone who is in a position to reveal information for the public good to be willing to destroy his or her career to do so.

25. It is an inevitable feature of being confidential informants that by disclosing the information they are doing something wrong in someone's eyes. Someone has deemed that information to be

confidential. By providing the information they are inevitably breaking some or other rule and are frequently risking criminal sanction. As is clear, they are thoughtful people, are aware of those risks, and balance that risk against the good they are doing in providing the information.

Importance of offering confidentiality

26. As noted above, the confidential informants I have dealt with frequently still maintain their public position. This extends to people holding the highest of public offices. It is absolutely essential to their ability to provide me with the information they have that I can guarantee them confidentiality.

27. In my mind there is simply no question. Were it not for a guarantee of confidentiality, many of the people who provide me with information would not do so. Were they not able to provide the information to the news media in confidence, a significant number of them would simply not feel able to provide the information to the public.

28. I have no doubt that there would also be an increasing number of other people who would chose to distribute the information directly to the public without going through the filter of the news media. One can already see this happening through such sites as WikiLeaks.

29. I am supportive of the general philosophic intent of sites like WikiLeaks – that sunshine is the best disinfectant. However, the news media have an important role to play as a filter of leaked material.

30. The news media do not simply parrot leaked material. The news media applies a rigorous process to information it receives from confidential sources. We do what we can to carefully fact check material and ensure the accuracy of material we are publishing. We seek to put material we do publish in its proper context. As noted

above, there are occasions where I have withheld publication as there were good reasons for doing so.

31. In my view, sites like WikiLeaks have published material they should not have published. There were some things published that did not have to be. There were names published of people who were talking confidentially to our state department. They were talking about things that were rational and good. It was contrary to the public good for those names to be exposed in that way.

32. Another possibilities is that a potential confidential informant may instead send information to the media anonymously. Documents provided in this was might appear to contain highly valuable information. However, it is almost never be able to be used. I do not know any responsible journalist who would make use of information when they did not know its source.

Impact on the availability of confidential informants

33. I understand that the New Zealand Police are seeking information about the identity of Rawshark. I also understand that in order to do that they wish to review essentially all of Mr Hager's correspondence including all of the material related to all of his other confidential informants.

34. It seems obvious to me that this will have an enormous detrimental effect on Mr Hager's ability to receive confidential information and on the ability of other New Zealand journalists to do likewise.

35. I appreciate that Rawshark is accused of a crime and I understand the legitimate interest that the Police have in investigating allegations of crimes. However, in my decades of experience every confidential source, without fail, has broken some rule or some law in providing the information.

36. I understand that Mr Hager's case has received public attention. As stated above, the confidential informants I deal with are socially engaged, intelligent people. They could be expected to be aware of what happens in a case like this. Given the nature of Mr Hager's work, which is in a similar field to my own, I would expect the same to be true of the type of confidential informants he uses.

37. In my view, the people who are considering whether or not to be confidential informants to the news media in the future will know and consider the outcome of this case. If the outcome is that it is lawful for the New Zealand Police to act in this way, then that will inevitably deter many people from being confidential informants. This is contrary to the public interest. It aligns instead with the interest of those who wish to continue to misuse claims of confidentiality to hide their malfeasance.

38. The result may be that potential confidential informants may choose to simply dump their information wholesale on the internet. If that happens, then it is my view that society is worse off without the filter provided by the news media. Others will simply not risk distributing the information at all, or try to provided it anonymously and in a way that means that the media cannot make use of the information. There will therefore be matters of significant public importance which I would expect would stay hidden because of the deterrence that this case will represent.

Opinion of Nicky Hager

39. Nicky Hager has produced a body of work whose importance will only grow with time. He was warning about intrusive government surveillance, without appropriate warrant, many years before the current revelations by Edward Snowden (important as they are).

40. Mr Hager's brand of fearless reporting is essential to democracy and to the sometimes uneasy peace that exists between the State and its citizens. I believe that it is essential for the well-being of New Zealand society that Mr Hager be allowed to continue doing what he does so well -- protect those whose information allows him to report on governmental abuse of authority.

41. We in the press who share Nicky Hager's values and purpose in journalism are appalled at the State action against him. I know Mr Hager. I know he is immensely proud of New Zealand and that he does what he does because of his love for New Zealand. That mirrors my own reason for my work for the love of my country.

Affirmed in Washington, District of Columbia, USA

by

Seymour Myron Hersh

this day of March 2015, before

LESLIE P. KIM NOTARY PUBLIC EXP. 8-31 2019 DISTRICT OF COLUMBIA

My Commission Expires
August 31, 2019
Leslie P. Kim
1718 M St. NW
Washington, DC 20036

SUBSCRIBE AND SWORN TO BEFORE ME
THIS 26 DAY OF March, 2015
BY Seymour Myron Hersh
NOTARY PUBLIC

a person authorised to administer oaths by the laws of the District of Columbia in the United States of America

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*

Affidavit of Gavin Peter Ellis

Dated: 31st March 2015

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

I, Gavin Peter Ellis, media researcher of Auckland, solemnly and sincerely affirm:

Introduction

1. I have been asked to provide this affidavit to assist the Court on matters relevant to the judicial review brought by Nicholas Alfred Hager in relation to a warrant issued to the New Zealand Police to search Mr Hager's residence and examine his documents and computer systems.

Code of Conduct

2. I have read, and agree to comply with, the Code of Conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules.

Experience

3. I hold the degrees of Master of Arts (First Class Honours) and Doctor of Philosophy in Political Studies from the University of Auckland. My specialisations are in journalism and the political economy of communication. I am a part-time senior lecturer in Media, Film, and Television at the University of Auckland, where I teach the structures, theory and practice of journalism. I am the author of peer-reviewed works on media institutions, ethics, and regulation. My 2014 book, *Trust Ownership and the Future of News: Media Moguls and White Knights* (London, Palgrave), addressed the need for institutional models that protect and foster journalism that contributes to civic life and democracy.

4. I have also practiced journalism for 50 years. In 2005, I retired as editor-in-chief of the *New Zealand Herald* after a 40-year career in daily journalism, during which I had practical experience with confidential sources and attempts by police to gather evidence from newsrooms. I now broadcast a weekly commentary on the media on Radio New Zealand National. I also write a bi-monthly column that addresses issues facing the news media and journalism for the *PANPA Bulletin* (an industry publication that circulates in Australia and New Zealand).

GPE
ACS

5. I was a founder member and former chairman of the Media Freedom Committee, which represents all mainstream media (newspapers, television, radio, and magazines) on matters relating to freedom of expression. In 2005 I was the recipient of the Commonwealth Astor Award for contributions to press freedom. In 2014, I acted as one of two independent advisors to the judicial panel reviewing in-court media coverage.

6. I act as a consultant on media matters and, as part of that consultancy, have peer-reviewed media codes of conduct and have been commissioned by a media company to investigate journalists' activities to determine whether ethical guidelines have been breached.

7. In 2009. I provided evidence as an expert witness in an application by the New Zealand Police seeking to compel TV3 journalist John Campbell and four other defendants from the television network to disclose the identity of an informant in a case that led to the prosecution of James Joseph Kapa and Robert Van Wakeren. My evidence supported the position that, with a very small number of exceptions, a journalist was bound to maintain confidentiality.

Background

8. I have met Mr Hager in the course of my activities at the University of Auckland and have utilised aspects of his work in lectures.

9. I am familiar with his book *Dirty Politics* published in 2014 and with the events that followed its publication, including subsequent disclosures to news media made by the person who identified himself as Rawshark and media reports of the execution of a search warrant on Mr Hager's home.

Instructions

10. I have been asked to assess the potential effects on journalists and their confidential sources of the raid on Mr Hager's house and of the possible access of police to his seized documents and electronic devices. The potential consequence of such acts is often called the "chilling effect". I have been

asked to examine the academic literature on the subject to determine whether, in conjunction with my own professional experience, it supports the view that denial of Mr Hager's application will have adverse consequences for him, the wider journalist community, and the public's interest in the news media's disclosure of important information possessed by potential confidential sources.

Overall opinion

11. In my view, the actions of the New Zealand Police in executing a search warrant on the home of Mr Hager – and the expectation that police officers will have access to the contents of his computer systems, documents, notebooks and other material relevant to his role as an investigative journalist – will have the following chilling effects. It will:

    11.1. act as a disincentive to potential sources because the journalist's solemn undertaking to maintain confidentiality is nullified by actions beyond the journalist's control;

    11.2. force journalists to adopt extraordinary time-consuming clandestine methods to protect sources' identities, or limit their dealings with 'whistle-blowers'; and

    11.3. compromise Mr Hager's ability to practice as an investigative journalist and his capacity to build vital trust with his informants by sending a signal that he is unable to protect the identity of confidential sources.

Principles

12. Before providing the reasons for this overall opinion, it may be helpful to set out what I believe are the underlying principles that are at stake in this matter. In so doing I will address not only the 'Reporter's Privilege' but the 'Reporter's Dilemma'.

13. The so-called 'Reporter's Privilege', often claimed and less often conferred, recognises a need for journalists to avoid identifying individuals who are

unable or unwilling to divulge matters of great public interest without a cloak of anonymity. It further recognises that journalists have a moral obligation to such informants to protect their identities (and, perhaps, employment and even freedom from harassment, vilification, retaliation or punishment) once an undertaking of confidentiality and been given.

14. It is a solemn undertaking that should not be made without considerable thought being given to whether or not it is justified. During my editorship at *The New Zealand Herald* I required reporters to seek the permission of a senior editorial executive (usually the editor) before giving such an undertaking. I required that the name of the source be made known to me

15. There are a number of 'tests' that can be used to determine whether a guarantee of anonymity – which precedes, and is not a guarantee of, publication – is warranted. I understand that Mr Hager has satisfied himself that his sources meet these criteria. The four questions that need to be asked are:

    15.1. Is this a matter of significant public interest sufficient to warrant a guarantee of confidentiality?

    15.2. Is confidentiality essential for the relationship between source and reporter to continue?

    15.3. Would the disclosure of the source's identity cause that person significant harm?

    15.4. Is the source acting in good faith?

16. If these tests are satisfied there must be a clear and unambiguous understanding of the agreement and a determination by all involved – the reporter and all others privy to the source's identity – to maintain confidentiality.

17. There are divergent attitudes on the validity and extent of legal protections for the 'Reporter's Privilege" but a general recognition that there is, at least,

some legitimacy to confidential sources where official wrongdoing or abuses of power cannot be revealed except by their use.

18. Within the English-speaking world there is a universal belief by journalists that confidential sources should not be revealed.[1] The inclusion of such a provision in codes of ethics is almost as widespread, as demonstrated by the attached matrix (Appendix A) that I developed during research on the commonality of journalistic ethics.[2] The entries relating to "Confidentiality" demonstrate that almost all significant journalistic codes of ethics contain a requirement to respect promises of confidentiality.

19. The burden on journalists is often stated unequivocally: The Editors' Code of Practice adopted by the Independent Press Standards Organisation in the United Kingdom (successor to the Press Complaints Commission) states simply that "Journalists have a moral obligation to protect confidential sources of information". Coulter's interpretation is that the journalist, once a solemn undertaking has been given, has no option but to maintain that secrecy come what may.[3]

20. Stone believes no offer of anonymity can legally extend beyond what is recognised by law[4] while others believe the agreement may be nullified by certain circumstances and that a balance must be struck. Martin-Clark, a journalist who broke such a confidence, justified his action by saying his disclosure of a confession of murder during The Troubles in Northern Ireland could have prevented further killings.[5] My own view, set out in my evidence in *Police v Campbell*,[6] is that there are only two circumstances in which the undertaking may be breached: (i) where a person or persons subsequently may suffer actual harm or a serious crime may be committed

---

[1] Weaver, D.H., "Who Are Journalists" in *Making Journalists*, H. de Burgh (ed). London, Routledge 2005. P. 83.
[2] Ellis, G.P., *Journalism's road codes: The enduring nature of common ethical standards,* Pacific Journalism Review, Vol 18 Issue 2 October 2012.
[3] Coulter, J., "The Moral Reason Never To Tell", *British Journalism Review* Vol 16 No 1 pp. 65-69.
[4] Stone, G.R., "Why We Need a Federal Reporter's Privilege" *HOFSTRA Law Review Vol 30:39, pp. 39-58.*
[5] Martin-Clark, N., "When a Journalist Must Tell", *British Journalism Review* Vol 14 No 2 pp. 35-39.
[6] Police v Campbell - [2010] 1 NZLR 483

unless the journalist discloses the source to appropriate authorities, and (ii) where there was an ulterior motive on the part of the informant in seeking confidentiality such as the publication of intentionally wrong information or the prevention of disclosure of self-incriminating material. At the other end of the scale, Wasserman regards the convention as "nothing more than a valuable information-gathering technique".[7] This is a view with which I strongly disagree, preferring the more widely-held opinion that it represents a valuable means by which wrong-doing and misuse of power, particularly by the state, may legitimately be brought to public attention.

21. But herein lies the Reporter's Dilemma: Journalists must of course act within the law but in order to satisfy their moral obligation to confidential informants set out in their codes of ethics – beyond the narrow band of exceptions outlined above – they may feel compelled to defy the law and risk the consequences.

22. There are numerous examples of journalists being prepared to go to prison rather than reveal a source. In the much-cited *Branzburg v Hayes* case (I have found Justice Potter Stewart's dissenting view useful in forming my views on confidential sources), the U.S. Supreme Court required journalist Paul Branzburg to reveal names to a Grand Jury. His continued refusal led to a six- month prison sentence.[8]

23. I was prepared for such an eventuality when, as editor-in-chief of *The New Zealand Herald* and before the addition of s 68 to the Evidence Act, I refused under lengthy examination to reveal the names of sources during an interlocutory hearing in the *Queen v Cara and Kelman*. In the event, I was relieved of the obligation to answer because the court found that the potential 'chilling effect' of my being forced to reveal the sources outweighed any benefit that might accrue to the defendants in that case.

---

[7] Wasserman, E.J. "A Critique of Source Confidentiality" *Notre Dame Law Journal*, Ethics and Public policy 553 (2005).

[8] Branzburg did not serve the sentence because the state to which he had moved refused to extradite him to Michegan.

24. A further principle in play here is the general duty on the part of a journalist to keep safe material utilised in published work or which may have informed those published efforts but which did not appear in print or go to air. This latter category might include background information that could lead to the identity of a source, the journalist's notes and observations (that could include potentially embarrassing musings about the character or activities of various related parties), recordings of interviews (far more fragmented and idiosyncratic than the polished and edited broadcast product and often with unguarded 'off the record' asides) and, importantly, material from other unnamed sources used to verify the informant's claims.

Reasoning

25. I would like now to return to my opinion of the effects that the execution of a search warrant on Mr Hager's home and the seizure of his computer equipment would have on him, journalists, and potential confidential sources. To reiterate, I believe there will be significant 'chilling effects' should the court unseal the considerable amount of material seized during a prolonged search of Mr Hager's home. I have formed my opinion on these matters for the following reasons.

26. I will assume (though I have no knowledge of this) that there is a possibility that forensic examination of the material could reveal the name of Mr Hager's confidential source or sources and thereby nullify the solemn undertakings he gave to maintain secrecy. I note that any police search would run the danger of unmasking confidential sources other than the one they are looking for. There is widespread belief among journalists that the revealing of a confidential source is a cardinal sin. An influential empirical study by Blasi in 1971 found that while many reporters felt testifying on sources to be a matter for personal conscience, there was "a very high level of asserted willingness to go to jail if necessary to honor what they perceive to be their obligation of confidentiality".[9] Coulter,[3] a political journalist as well as being a senior lecturer in journalism, asserts that journalists "...have

[9] Blazi, V., "The Newsman's Privilege: An empirical study", *Michegan Law Review* Vol 70:229.

a moral imperative to give a guarantee of anonymity to genuine confidential sources providing bona fide information" and further asserts that if journalists sacrifice the trust implicit in that relationship, "we betray our credibility as reporters of the truth".

27. I believe Police access to material in an attempt to identify his informants will lead to Mr Hager being seen as unable to protect his sources and other journalists taking the view that they are similarly vulnerable to search and seizure that could expose their own confidential sources.

28. The ability to protect sources who take risks to provide information, the disclosure of which is demonstrably in the public interest, is a cornerstone of investigative journalism. If potential sources feel journalists are no longer in a position to honour guarantees of confidentiality they are left with two options: to make the information public and bear the consequences of exposure as the source, or to stay silent. There are compelling incentives to stay silent, given that an informer may lose his or her livelihood and be charged with theft for handing over even material revealing the most egregious wrong-doing by the state or a corporation. Whistle-blower protection in the Protected Disclosures Act is, at best, a limited shield as it maintains a closed circuit within the organisation and referral upward and leaves the whistle-blower within a power structure that may be perceived as intimidating or hostile. Nor does it even guarantee anonymity to the whistleblower. The ability to 'go public' remains an important safeguard in a democracy.

29. Equally important is the ability of journalists to access multiple sources to verify stories. Kovach and Rosenstiel say the essence of journalism is a discipline of verification – checking and cross-checking in order to get it right.[10] Any reduction in the level of confidential sources' trust in journalists reduces the ability to find sources who will confirm facts on an anonymous basis. Information from confidential sources may well be of such a nature

[10] Kovach, B., and T. Rosenstiel, *The Elements of Journalism* 2001, New York, Three Rivers Press.

that other knowledgeable people will only confirm matters under a similar guarantee of anonymity offered to them.

30. In *Police v Campbell* the judge was asked to exercise his discretion under s 68 of the Evidence Act 2006. The judge held that, in the circumstances of that case, the public interest in the disclosure of the identity of the sources outweighed the public interest in the communication of facts and opinion to the public. He referred to evidence that the chilling effect may be less when the case is not high-profile, the courts do not force disclosure frequently, and other sources do not see themselves as being in a comparable position. He concluded that the public interest in the disclosure of identity was high, and the likelihood of harm to the public interest in ordering disclosure was low, because of the very unusual circumstances of the case (which involved a self-confessed thief of valuable medals) and the low incidence of similar court orders. I believe the current case is significantly different (and much more in line with the disclosure cases encompassed by the literature) because *Police v Campbell* involved a self-incriminating common thief and not a 'whistle-blower' (as I consider Rawshark to have been), it was not a matter that impacted on the public beyond a sentimental attachment to war medals, and the circumstances may have been unique. Nevertheless – and in spite of the judge's assurance that compulsion under s 68 would be infrequent – I believe that, should the court unseal Mr Hager's material, the cumulative effect will be to persuade journalists that they should not rely on the section to protect their sources. It will add to a growing list of assaults that journalists see being made on media freedom such as 'witch-hunts' over leaks, search warrants, and the collection of electronic metadata.

31. The majority decision in *Branzburg v Hayes* rested, in part, on the view that there was no empirical evidence to support the claim that enforced disclosure would have a chilling effect on sources. Justice Stewart's view, however, was that the court had never before demanded that First Amendment rights rest on elaborate empirical studies demonstrating beyond any conceivable doubt that deterrent effects exist. I believe that to

require such proof before acknowledging a 'chilling effect' is counter-intuitive: how can one build a body of evidence that undisclosed sources decided to stay silent? In any event, there *is* evidence that invasion of the reporter's ability to protect sources has led to sources 'drying up' and important information in the public interest suppressed. In 2005, as reporters from the *New York Times* and *Time* magazine faced imprisonment for refusing to reveal sources of stories in the build-up to the invasion of Iraq, the *Cleveland Plain Dealer* withheld two investigative articles that the editor Douglas Clinton described as "profoundly important" for fear that the sources would be identified and imprisoned.[11]

32. Following the seizure of telephone records of The Associated Press by the US Department of Justice in 2013, the wire service's chief executive, Gary Pruitt, stated that "some long-term trusted sources have become nervous and anxious about talking to us – even on stories unrelated to national security… this chilling effect on newsgathering is not just limited to AP. Journalists from other news organizations have personally told me that it has intimidated both official and nonofficial sources from speaking to them as well."[12]

33. It is reasonable to believe that journalists have already been unsettled by the events surrounding the seizure of Mr Hager's material and computer systems. It has been widely reported[13] that Police spent 10 hours at Mr Hager's home in his absence. Journalists in New Zealand find the execution of search warrants on newsrooms unsettling because it is seen intuitively as a violation of press freedom.[14] To now feel that their homes may also be

---

[11] McFadden, R., "Newspaper Withholding Two Articles After Jailing", *The New York Times*, 9 July 2005.

[12] Pruitt, G., Address to the National Press Club 19 June 2013. Retrieved from http://www.ap.org/Content/Press-Release/2013/Gary-Pruitt-address-to-National-Press-Club

[13] http://www.stuff.co.nz/national/10585208/Nicky-Hagers-house-raided-by-police http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11337913 http://tvnz.co.nz/national-news/nicky-hager-i-d-go-jail-before-revealing-dirty-politics-source-6099688

[14] During the Teapot Tape investigation in 2011 – which followed the recording of a conversation between Act leader John Banks and National Party leader John Key in an Epsom café – search warrants were executed on the premises of the *Herald on Sunday*, TVNZ, TV3 and Radio New Zealand, leading to much public debate and concern about press freedoms

subjected to such intrusion adds an altogether more personal dimension. An increasing number of journalists work from home and those writing on sensitive subjects may now feel they are putting the well-being of their families at risk.

34. Journalists must protect confidential sources and material and there is already some evidence that journalists are going to extraordinary lengths to protect sources in the wake of (i) revelations that the telephone records and parliamentary movements of Dominion-Post reporter Andrea Vance had been accessed during the investigation into the source of the leaking of the Kitteridge report into the activities of the GCSB in 2013 and (ii) disclosures by former U.S. security contractor Edward Snowden of GCSB surveillance operations. The measures being taken by journalists include:

34.1. non-use of the parliamentary telephone system for sensitive calls,

34.2. the use of so-called 'burners' – cheap, pre-paid cell phones with no ownership record that are used briefly then discarded; and

34.3. the use of encrypted email.

35. I regard these measures as a form of 'chilling'. They are symptomatic of the need for journalists, already under substantial pressure as a result of reduced numbers in newsrooms and increased workload in a multimedia digital environment, to add significantly to the processes involved in their occupation in order to honour their undertakings. I am aware of journalists in New Zealand who, in addition to the measures outlined above, employ elaborate means to protect their sources and to keep their on-going investigations secret. These measures include removing themselves from conventional Internet and email communication, which in surveillance circles is known as 'going dark'. It involves placing all online communication on what is known as the "Deep Web", a series of hidden networks predicated on anti-surveillance protocols. It is telling that, in order to prevent surveillance and disclosure, journalists are prepared to use networks that are also utilised by criminals, terrorists, and paedophiles.

GPE

Publications such as *Deep Web for Journalists: Comms, Counter-surveillance, Search* by Alan Pearce instruct journalists on how to take themselves into this clandestine environment. These networks were used by Edward Snowden in his communications with the editorial team led by Glenn Greenwald. It is noteworthy that the initial contact broke down because Greenwald was unable to set up the counter-surveillance software that Snowden demanded. Entering this Deep Web is time-consuming and complex.

36. At the other end of the scale is a return to reporting methods that pre-date the introduction of the telephone. The Australian chief executive of Rupert Murdoch's News Corporation, Julian Clarke, has warned journalists in his organisation to stop using text and email messages and meet sources face-to-face in light of new laws on the gathering and retention of electronic metadata.[15] Of course, this makes it much more difficult to meet with sources from out-of-town, particularly if the journalist is determined not to create any trail of the contact.

37. The use of such strategies is confirmed in a 2014 report by the American Civil Liberties Union and Human Rights Watch,[16] which found that fear of surveillance and the compromising of sources had led journalists to adopt three defensive strategies:

    37.1 use of advanced privacy and security technology;

    37.2 decreased reliance on digital technology; and

    37.3 use of other strategies such as diversionary tactics including the laying of false digital trails.

38. Investigative journalism is an expensive undertaking that requires journalists spending weeks and sometimes months on a story. Anything that adds to the burden of the investigative journalist ultimately translates into a reduced output. This, coupled with minimal editorial budgets, leads to hard

[15] Markson, S., "Julian Clarke: texts, emails out for journalists' sources", *The Australian* 23 March 2015.
[16] ACLU/Human Rights Watch, "With Liberty to Monitor All: How large-scale surveillance is harming journalism, law, and American democracy". Downloaded from http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf

decisions on how many investigative projects will be undertaken. In *Trust Ownership and the Future of News* I lamented the reduction in what I described as democratically significant journalism. This can only be exacerbated by further impediments to the ability of investigative journalists to do their jobs.

39. A further 'chilling effect' lies in the subject of Mr Hager's investigation, which was firmly rooted in domestic politics. Journalists acknowledge that government has a responsibility to maintain national security – although they may be highly critical of inappropriate actions taken in the name of national security. Journalists are certainly mindful of the responsibility of government, and their own obligations, in the face of threats to national security. However, when the security of the state is not at risk and there is clear public interest in the disclosures being made, journalists begin to worry when their ability to do their job is impeded by the power of the state. I believe journalists will regard this case as a sea-change, a perilous shift that places coverage of politically sensitive domestic issues in the same area of "risky" coverage as national security. Journalists may well ask themselves whether they should be more cautious in writing on politically embarrassing subjects that almost invariably will involve unauthorised access to material. That is not a question that should need to be posed in a free and democratic society.

40. Finally, I turn to the effect on Mr Hager should Police gain access to his material – even if it does not, in fact, reveal the identity of his sources.

41. I have no doubt that Mr Hager will continue in the role of investigative journalist and will seek to cultivate existing and new confidential sources. However, there will be inevitable consequences for him, as follows:

    41.1. He will feel compelled to go to even more extraordinary lengths to protect his sources and the integrity of the material he holds.

    41.2. The time-consuming nature of the security measures he will feel compelled to implement will affect his productivity and, hence, his income.

PE

41.3. While his confidential sources may not blame him directly for any breach of confidence he will be forced to rebuild the level of trust they have resided in him.

41.4. Potential sources that may have approached him could now be reluctant or unwilling to do so.

41.5. He may be faced with the prospect of sources refusing to identify themselves to him (a dangerous situation open to malicious manipulation and one that I would not countenance when I was a editor).

41.6. He may be forced to shoulder the added expense of office accommodation to avoid exposing his family to the anxiety of potential future searches of his home.

Summary

42. I am firmly of the view that to condone the Police search of Mr Hager's home by unsealing the computer systems and materials seized in that search will have detrimental consequences for him and for society at large that outweigh whatever benefits that may arise from police examination of the material.

GPE

GCD

104

Appendix A

	U.K. Press ComplaintsCom.	National Union Journalists U.K.	New York Times	Los Angeles Times	Associated Press (U.S.)	Brit. Columbia Press Council	#Canadian Newspaper Ass.	Australian Press Council	New Zealand Press Council
Accuracy	•	•	•	•	•	•	•	•	•
Attribution			•	•	•				
Balance			•	•	•		•	•	•
Children	•			•	•	•			•
Confidentiality	•	•	•	•	•	•		•	•
Interest conflict	•	•	•	•	•	•	•		
Correction	•	•	•	•	•	•	•	•	•
Discrimination*	•	•				•		•	•
Fabrication**		•	•	•	•				
Fairness		•	•	•	•		•	•	•
Grief/shock	•	•						•	•
Harassment	•		•						
Identification	•		•	•	•	•			
Privacy	•	•	•		•	•	•	•	•
Right of reply	•		•	•	•	•	•	•	•
Sex victims	•			•	•	•			
Subterfuge	•	•	•	•		•		•	•
Treating			•	•	•				

• Includes communal tension ** Includes plagiarism
Individual Canadian newspaper codes include confidentiality provisions.

Affirmed at Auckland)
on the 31st day of March 2015)
before me)

GARRY CLAUDE WILLIAMS

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

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*

Affidavit of Adam Julian Boileau

Affirmed: 2nd April ~~March~~ 2015

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

I, Adam Julian Boileau, computer security consultant of Wellington, solemnly and sincerely affirm:

Introduction

1. I have been asked to provide this affidavit to assist the Court on matters relevant to an application for judicial review brought by Nicolas Alfred Hager in relation to a warrant issued to the New Zealand Police to search Mr Hager's residence and examine his documents and computer systems as part of an investigation of a person who leaked data to Mr Hager and who has been using the alias Rawshark (the "**Leaker**").

Code of conduct

2. I have read the code of conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules. I agree to comply with it.

Instructions

3. I have been instructed that it will be relevant to the Court's assessment of this case for the Court to understand:

   3.1. whether the Police had avenues of investigation into the identity of the Leaker which they could have explored instead of seeking to search Mr Hager's property; and

   3.2. what were the prospects of the Police finding evidence of the identity of the Leaker from a search of Mr Hager's property.

4. In the course of giving advice on these matters to Mr Hager's legal team, I was also asked some specific follow up questions which I address in the text below.

Qualifications as an expert

Experience

5. I have 15 years of experience working in the field of computer security. For the last 10 years I have been working as a computer security consultant. I

am currently the principal consultant and part owner of Insomnia Security, a computer security company with offices in Auckland and Wellington and with a current staff of 18.

6. My work primarily involves understanding how to obtain unauthorised access to computer systems. I do this for clients either to test and improve their security precautions, or to aid them in identifying the source of breaches in their computer security. I also assist in training the staff members of private organisations to detect and protect against security breaches.

7. In addition to my work, I am active in research, public commentary, and conference organisation in this field.

8. I am the news analyst for the weekly information security podcast Risky Business, a regular information security news audio program started in 2007. I am a regular commentator on computer security issues on mainstream media including National Radio and TV3. In my role on Risky Business, I am a three times winner of a Lizzies Award, the leading award recognising information technology journalism and media in Australia and New Zealand (2010 "best publication", 2011 "best audio program", and 2012 "best audio program").

9. I am one of the owners and key organisers of Kiwicon. Kiwicon is New Zealand's only computer security conference and the largest in Australasia. The conference was run for the 8th time in 2014.

10. My original published research includes work on the "Firewire" technique of computer memory acquisition for forensic purposes. That work has been used in "Volatility Framework", the leading open source digital forensic tool for the analysis of computer memory. I have also presented a variety of papers at a number of computer security conferences and at industry presentations, and have received high praise for that work.

11. I have an Advanced Diploma in Business Computing (Auckland University of Technology, 1998). Very few formal qualifications existed in

this industry, especially in the 1990s. As a result, I, like essentially all of the leading experts in my field, have expertise through work experience more than through academic training.

12. In 2014, Kiwicon won the inaugural iSANZ Hall of Fame Award for making a significant contribution to the New Zealand's information security industry. That award is judged by industry peers including a member of the Government Communications Security Bureau.

Forensic work and computer crime

13. I make a distinction between forensic work in this field and non-forensic work. Using "forensic" in this way, I mean work where the results of the work are intended to be used in a criminal court.

14. The majority of my experience has not been in forensic work in this sense. I have an understanding of forensic principles, but my clients have principally been private organisations seeking either to ascertain the nature of a security breach or else to prevent one from occurring. However, through my work, I am very familiar with the methods for identifying the source of a security breach of the kind that was alleged to have occurred in this case.

15. Therefore, the question, "what else could the police have done to identify the source of the leak?" is within my field. But, I would not claim to be expert in carrying out the enquiries myself so as to preserve the chain of evidence for use in a criminal Court.

16. I am aware that some people used the phrase "a forensic examination of a computer" to mean an in-depth examination to reveal information that the user of the computer may not have been aware was there, irrespective of whether the results are going to be used in a criminal court. As explained above, this is not consistent with the way in which I use the word "forensic". To be clear, I am an expert in the techniques involved in these types of examinations of computers.

17. In understanding expertise in this area, I believe it is also important to distinguish between *computer crime* – breaches of the laws relating to the use of computers – and *crimes involving computers* – any crime, but where the perpetrator has used a computer in the course of committing the crime. This case involves a computer crime. My expertise is in the area of computer crime, or the complementary area of computer security – in other words prevention of computer crime.

18. Computer crime is less prevalent than crimes involving computers. For this reason, most people involved in forensic work spend most of their time dealing with crimes involving computers rather than computer crimes. People who specialise in forensic work involving computer crime are rare.

19. As I explain below, there were a number of basic things done very badly in this investigation. Given the nature of those errors and given my specialist knowledge of computer crime, my view is that the reason that these errors were made was because those in charge of the investigation were not expert in computer crime. The steps taken indicate that the investigators were treating this as they may treat any crime involving a computer without sufficient understanding of the particular requirements of investigating a computer crime.

Concerns raised by the Police

20. I have been told that my access to disclosed documents was challenged by the Police based on unspecified comments I made at last year's Kiwicon.

21. As explained above, I am one of the owners and organises of Kiwicon. I also acted as the master of ceremonies for the 2014 conference. Kiwicon, like its overseas equivalents, plays up the risqué aspects of the field. Such conferences describe themselves as "hacker conventions" and many of the participants style themselves as "hackers".

22. The use of the term "hacker" does not means that those people engage in unlawful activity. People in this industry do not use the term "hacker" to exclusively denote someone who engages in unlawful activities. Rather, it

is generally used by many to denote anyone in this field. People in this field may work in law enforcement and still regard themselves as a "hacker".

23. That said, the industry also likes to make light of the reputation of hackers as law breakers. Kiwicon is no exception. The conference also makes use of a great deal of tongue-in-cheek humour.

24. Notwithstanding that manner of presentation, Kiwicon is a serious conference. It involves the discussion of serious matters of computer security including highly technical matters. The attendees and participants include leading figures in the industry including many people from law enforcement. We had attendees at the last conference from the New Zealand Police and from the Government Communications Security Bureau, as well as attendees from overseas law enforcement agencies.

25. *Dirty Politics* and the surrounding stories about the Leaker were highly topical at the time of last year's conference and were relevant to the field of computer security. The call for papers made light of the Leaker and talked about the skill he had displayed as a hacker. It was a running joke through the conference that "Rawshark" was going to put in an appearance at the conference. The Leaker was a constant source of comments, both serious and comical.

26. A supporter of Mr Hager brought "I AM RAWSHARK" t-shirts to the conference and asked if they could be sold to raise money for Mr Hager. I was not involved in the sale of those t-shirts, but I gave permission for them to be sold at the conference and, as MC, I informed the conference that they were for sale.

27. Many people in this industry have a chequered past. When young, they may have tested their hacking skills by trying to gain unauthorised access to a computer system and have been caught. I am not one of those. I have never been in trouble with the law. I am "known to the police" only because they regularly attend the conferences I run.

28. As I will explain further below, I believe that the Leaker has demonstrated, through some of his actions, a reasonable degree of competence in the use of information security techniques. I have publically stated as much. I also think that it was a good thing that the immoral acts that were exposed in the book *Dirty Politics* were exposed. However, that does not mean that I support the Leaker's actions in breaking the law. I am a law abiding citizen. My work is devoted to helping people protect themselves from unlawful intrusions.

Background understanding of the case

29. I have been provided with documents which I am told constituted all of the documents provided to Mr Hager by the Police in the course of this proceeding and in response to all related Official Information Act and Privacy Act requests, except for documents or parts of documents that I was not permitted to see by order of the Court. I have reviewed all of these documents. I understand that a complete set of those documents is being produced as "Police Disclosure" volumes. Henceforth, I refer to documents from those volumes as **PD [volume number]/[page number]**.

30. I followed the background matters in this case as they unfolded. I took a particular interest in them at the time given the suggesting that the case involved computer crime. I have also read *Dirty Politics*.

31. I understand that Mr Hager says he based the contents of that book on correspondence given to him by a confidential informant, the Leaker. I know that it is alleged that the Leaker procured that correspondence by accessing a computer system without authorisation, which is a criminal act in New Zealand. I understand that the Police are investigating that alleged crime and that that is the purpose of the warrant.

32. I have elected to refer to this person in this affidavit as the "Leaker". I am aware that he goes by the alias "Rawshark". Many people have been referring over the last few months to "the hacker known as Rawshark". I expect that I may have said that myself. However, I am now charged with

giving a professional view that requires me not to make assumptions about what took place. I therefore do not want to use a term that presupposes what occurred. It may be the case that the Leaker obtained the information he leaked by obtaining unauthorised access to Mr Slater's computer. All I know for sure is that he leaked the information to Mr Hager.

33. Lastly, I am aware that Mr Hager is challenging the legality of the warrant in these proceedings, chiefly on the ground that the administrative processes leading up to it failed to take account of the public interest in him being able to protect the identity of his confidential sources.

Reason for IP photo

34. During my work on this file I was asked to consider the photograph appearing at **PD 7/1407**. I am told that this is a photograph of a laptop that the Police agreed to clone, and for the clone to be sealed pending the decision of this Court. I noted that the events surrounding the taking of this photograph appeared to be set out in a statement from ECL Officer Ian Donovan at **PD 8/1585**.

35. The first question posed to me was whether the taking of that photograph formed any part of the cloning of the laptop. My answer to that is unequivocally, no. There was no legitimate need to review the information seen on the computer screen as part of a cloning process, and additionally, no need to record it.

36. The second question was, if not, then could I explain why the Police took this photograph. Reviewing the statement identified above, I believe the answer is clear. A Member of the Police wanted to access Mr Hager's internet connection. I do not know why they did not have an internet connection of their own. I would have expected them to have their own portable access to the internet. As they had the laptop in their possession for the purpose of cloning, they decided to interact with the laptop to cause it to display the information that can be seen in the photo. That information

provided them with the details they needed to connect to Mr Hager's internet connection.

Confidential email

37. I have reviewed the email which is at **PD 7/1223**. I understand that it has been suggested that this email contains secret police investigative techniques in relation to computer security. For that reason, disclosure of the document to me was opposed. I was only permitted to see this document after signing an undertaking not to make any use of it outside of these proceedings. In my view, this email does not contain anything that could sensibly be regarded as a secret police technique. Some people will not know one or more of these things. However, all of the matters discussed in this email are able to be known by anyone seeking that knowledge from publically accessible sources. They were certainly all well known to me, as they would be to any competent computer technician, let alone any computer expert.

What else could the Police have done?

Methodology

38. I agreed to assist on this case a long time before I was provided with the documents disclosed by the Police. In the absence of those documents, I began by making a list in the abstract of what steps I would expect to take in a case of this kind in order to determine what took place and to identify the Leaker.

39. Once I received the documents, I familiarised myself with them. I considered whether the information that the Police had varied the steps that I thought were appropriate to take. I checked to see which of the steps I had identified had been taken.

Overall impression

40. As I will explain in more detail below, the Police in this case failed to do the most basic and most important steps in an investigation of this kind.

The investigation as a whole appears to have been a large one. It involved a large number of Police personnel. A significant amount of resources from the Electronics Crime Lab and the National Cyber Crimes Centre appear to have been made available to this investigation. And yet, the steps that should have been the highest priority – those most likely to have revealed the identity of the Leaker – were all but ignored.

41. The steps that were taken in relation to investigating computer systems include some basic steps that might be expected in the case of a crime involving computers. However, the investigators did not seem to pursue many avenues of investigation related to the nature of the crime itself, a computer crime.

42. The steps I say were the most important were steps I identified before I had seen any of the papers. My review of the documents that the Police provided had reinforced the view that these were the avenues of investigation most likely to identify the Leaker. That these were the correct steps to take should have been known to anyone competent in the field of computer crime. Indeed, in my view many are common sense steps that should have been obvious to anyone without any particular expertise.

43. I am aware that the Police have withheld various documents. It is possible that those documents show that the Police took steps of which I am unaware. However, for reasons I will explain, this appears unlikely in relation to at least some of the steps. In any case, I have been asked to give my opinion based on the documents with which I have been provided.

People with access

44. Before conducting an investigation on the assumption that someone had somehow bypassed Mr Slater's computer security, I would have expected the Police to follow up with anyone who had been granted access to this data for some other purpose.

45. Whenever one is investigating a leak of information from a computer system one needs to consider both the possibility that the person who

leaked the information was an "insider" and that it was someone "external". By insider, I mean someone who had been granted some level of access to the computer system and was misusing that access. An external person would be someone with no access who is doing what would be commonly described as hacking.

46. In general, insiders must overcome a much lower technical barrier to obtaining information. They may already have all of the access they need to obtain the information and merely need to misuse that access. If they need more access, the access they have already may make getting the additional access easier than it would be for someone with no access. External people hacking a system require a great deal of technical expertise.

47. When commencing an investigation into a security breach of this kind, one of the first things that any competent person would do is to try to establish a complete list of everyone who had been granted access to the system either currently or in the past. There is nothing in the documentation that has been provided to me to suggest that this occurred. Furthermore, there are signs in the documents that obvious leads, of people who ought to be on that list and who ought to have been investigated at the outset, were ignored.

48. One of the Police reports notes an interview with [redacted] That report is at **PD 7/1376**. Mr [redacted] set up the whaleoil.co.nz website on the web-hosting server. He noted that he had a limited technical background. As a result, he made use of other people to set up the website. Such other people are almost certain to have been provided with access that would have enabled them to access the data that was leaked. However, there is no record of the Police seeking the names of such people or following up with any investigation of them.

49. One would also expect the Police to consider the possibility that the Leaker was a member of staff of whaleoil.co.nz or a contributor or moderator to that site. By a contributor, I mean someone who is able to post stories as an article in the main body of the blog as opposed to a commenter who sends

in an unsolicited response to an article. A moderator acts like a sub-editor on a blog site. Specifically, they are tasked with reviewing comments before they are permitted to be loaded onto the site. Staff members, contributors or moderators may well have been given access to whaleoil.co.nz that could have been exploited to obtain the leaked information.

50. A quick review of whaleoil.co.nz revealed the name of [redacted]. Mr [redacted] is described on the site as a member of the whaleoil.co.nz staff and he describes himself as a moderator. He has also posted articles variously described as being as a contributor or staff member. I have seen no mention of Mr [redacted] name in any of the documents that I saw or any suggestion that he had provided information that had been withheld on the grounds of confidentiality. As I will explain below the Police had other reasons to want to talk to Mr [redacted]

51. I don't know who else would fall into the category of staff members, contributors, or moderators of whaleoil.co.nz. However, there is nothing in the documents to suggest the Police made any efforts to find out.

52. Next, one would consider anyone else who had physical access to Mr Slater's computers: anyone who had provided IT assistance, Mr Slater's family, the cleaner. The most basic first step would have been to sit down with Mr Slater and make a list of such people. There is nothing to suggest that this was done.

53. There is a related story that illustrates this point well. In *Dirty Politics*, Mr Hager made use of material from David Farrar's company. Mr Farrar publicly complained that that information could not have come from Mr Slater. Mr Farrar suggested that he too had been hacked. However, Russell Brown, a public commentator, later pointed out that the information was a leak from a staff member, not a hacker. I do not know whether any of this is true. However, it illustrates the point that one needs to investigate insiders as prime suspects for any leak.

The scene of the crime

54. The next most obvious step is to investigate the scene of the crime. In relation to an alleged computer crime of this kind, that involves examining the computer systems that are said to have been compromised. In this case, the allegation is that the Leaker accessed Mr Slater's private information held by Google, Facebook, and on the www.whaleoil.co.nz website. The confirmed scenes of the crime would be the systems of Google, Facebook and whaleoil.co.nz, and while no direct evidence exists to confirm it, potentially also the personal computers and phones of Mr Slater.

55. With respect to these three confirmed sites, the most important one to thoroughly examine in this case, for reasons I explain below, was whaleoil.co.nz. That was also the site to which the Police had potentially the greatest access and the most avenues of investigation. Yet, the Police made very little effort to examine that website.

56. We know that the Leaker had access to whaleoil.co.nz. David Fisher of the NZ Herald reported that he had been provided by the Leaker with a file giving the IP addresses of people posting comments on the website. That report is at **PD 5/870-871**. An IP address is a string of numbers which identify a computer, at a particular point of time, to other computers with which it is communicating. It may be useful in identifying a computer user, but there are ways to mask ones identity some of which are discussed below.

57. Mr Fisher's report revealed, amongst other things, that the Press Secretary of The Hon Gerry Brownlee had made a comment on the website congratulating Mr Slater for his attacks on Simon Pleasants. The Press Secretary eventually admitted making the comment. This confirmed one of the allegations in *Dirty Politics*. It also confirmed the accuracy of information provided by the Leaker which could only have come from the

website, either directly or via indirect means such as from back-up copies of the website data.

58. In his complaint to the Police, Mr Slater points out that this information could only be obtained from the comments logs on his blog. A redacted version of that complaint is at **PD 8/1441-1452**. The IP address information is held on the computer that operates the website, but is not something that is accessible by people viewing the website over the internet.

59. The Leaker therefore had access to whaleoil.co.nz. One needs to consider how this could have occurred. Assuming that the Leaker is not an insider, an investigation of this crime would start by considering the most likely points of entry – the most likely weak points in the security of the site – and checking for evidence of entry at those points that might divulge the identity of the Leaker. For a site of this kind, that would involve checking with the hosting provider that operated the computer and network services, the domain name registry, the name hosting service for the website's domain name, and examining the data for the website itself.

60. I note that the Police contacted Google and Facebook and requested information about access to Mr Slater's account (**PD 4/493, 539, and 627-637**). The Police also contacted internet service providers and requested subscriber information in relation to access records provided by Google and Facebook. Lastly, the Police contacted Linode, the company that had been providing the web-serving computer and internet service that ran the www.whaleoil.co.nz website (**PD 7/1387**). However, as explained below the enquiries with Linode were wholly inadequate.

Initial scene

61. There are a lot of reasons why it is likely that the Leaker's initial point of access was through whaleoil.co.nz. In computer crime, it is often particularly helpful to examine the scene of the first crime. This is because it is common for computer crimes to often begin as opportunistic crimes

with a person exploring without a particular intent. To use the colloquial – messing about, or trying their luck.

62. It is likely that the person was targeting Mr Slater. But it is possible that they began with limited expectations of being successful. Often this is how computer crimes begin, and while people are just trying their luck they are often much less careful about protecting their identities.

63. There are two reasons for this. First, when people are just messing about they are much less conscious that what they are doing is criminal and needs to be hidden. It probably is criminal, or at least an attempted crime, but because they do not necessarily expect to actually gain access and obtain information they do not take the risks involved in their activities as seriously. Once they know that they have access, and are logging in with the intent of downloading private data, they are generally much more conscious of the need to do so anonymously.

64. Secondly, successfully accessing a system anonymously requires a reasonable degree of discipline, and it also creates inconveniences. Experienced computer users usually sit at a computer with multiple programmes and windows open and switch between different activities. They might be writing some computer code in one window and chatting to a friend in another, or perhaps using the Netflix account to watch a movie in a third, or perhaps be logged into an online game. If you want to access a computer system in an untraceable way you cannot do this. You might use what would otherwise be an untraceable IP address to gain the unauthorised access, but then use the same IP address in relation to your personal email account. A truly untraceable intrusion therefore requires one to use a computer system running nothing that could possibly identify the user. In the industry this is known as "silent running".

65. If one has already succeeded in stealing a password, then it is one thing to use the password to gain unauthorised access and download data while silent running. It is quite another thing to be silent running for hours, or

days, on end while one researches and tries multiple different ways to access a system without a necessary expectation that any attempt will work.

66. So someone investigating a computer crime will pay particularly close attention to the scene of the initial entry. As stated above, I think there is good reason to believe that in this case that is the www.whaleoil.co.nz website.

67. First, the website used a software package called WordPress. WordPress has historically been subject to a number of security breaches caused by poor quality security measure in its software. There is an online database called the common vulnerabilities and exposures database hosted by a US defence contractor called the Mitre Corporation (cve.mitre.org). This is regarded as the authoritative source for recording discovered software security vulnerabilities. Since 2003, there have been 851 distinct vulnerabilities identified in WordPress and its related software. There is another website, wpvuldb.com (short for WordPress Vulnerabilities Database) which is dedicated to just listing the vulnerabilities of this software.

68. As a result, there are a number of hacker tools that have been developed to assist people to gain unauthorised access to WordPress websites. These are pieces of software which are programmed to assist someone trying to gain such access by exploiting established security flaws.

69. Using WordPress software is regarded in the industry as a "kick me". The equivalent of a school boy having a piece of paper with the words "kick me" written on it stuck on his back. I do not wish to be read as supporting that sort of an attitude to other people's private data (or to bullying school children). I do not. However, this is an attitude that is prevalent.

70. Secondly, the www.whaleoil.co.nz website was set up by someone who, as noted above, admitted himself that he did not really know what he was doing. This means that he may have installed software incorrectly in such a way as it created a security hole. It also means that the site is unlikely to

have been maintained properly in a way that ensured its ongoing security. Additionally, it means that more people needed to be involved in working on the system, which means that more people had access.

71. Thirdly, in response to the denial of service attacks, some technical changes were made to the www.whaleoil.co.nz website to make it more resistant to such attacks. These changes would have likely been made with limited opportunity for planning, under significant time and publicity pressure, and by Mr Slater and Mr [redacted] who lacked technical experience in making such changes. Security flaws are often introduced or exposed during hasty and unplanned changes.

72. Fourthly, as noted above, the www.whaleoil.co.nz website was hosted by Linode. Linode also has a chequered security history. There have been a number of well-publicised occasions in recent years during which that company has been successfully attacked for the purpose of accessing its customers' data. Linode has admitted such breaches. Its website contains reports, for example, of breaches in April 2013, January 2013, and April 2014. I would not single them out for criticism based on the third of those examples which was a common security flaw across the internet. The other two were Linode specific problems.

73. Lastly, the other known points of intrusion are Google and Facebook. These are two of the Internet's giant companies. They have enormous security budgets and skilled security staff. It is not impossible that someone gained access directly through those companies, but comparatively it is much more likely that access was gained through the www.whaleoil.co.nz website. It is highly feasible that access to Facebook and Google accounts was achieved through the use of data obtained by first breaching the security of whaleoil.co.nz.

74. A person with some technical acumen can use control of a website or domain-name to escalate this into access to other services, such as gmail (the Google email service that was accessed in this case) or Facebook accounts, through a number of means. A simple example would be taking

a copy of the password used to log into the administrative portion of the website and attempting to reuse this password to access other services. This will work if, as is commonly the case, the user is using the same password for multiple services. An example of a more advance technique would be to use the trust placed in the website by its owner to break into their desktop or laptop computer through malicious software. This could be done, say, by sending a message that will appear to come from the website software reading, "Wordpress has been updated; please download and install the following file to maintain compatibility".

75. All of this suggests to me that the most likely initial site of the security breach in this case was the www.whaleoil.co.nz website. That site should therefore have been the focus of the investigation. Instead, it was barely investigated at all. Even if the www.whaleoil.co.nz website was not the initial scene of the crime, we know, as explained above, that it was a scene of the crime. That alone means that all of the steps explained below should have been taken.

The web-host

76. While the Police did contact the company hosting the computer and network service for the www.whaleoil.co.nz website, Linode, their enquiries were limited to matters involving the denial of service attack on www.whaloil.co.nz. The enquiry was far too limited. There was also no follow-up to the information that Linode did supply. The sort of enquiries that should have been made are things that might not be something that one would consider in a crime involving a computer. However, they were the most basic and obvious steps to take given that this was a computer crime.

77. In his statement, Mr Slater alleges that the www.whaloil.co.nz website had been subjected to a denial of service attack. Mr Hager suggests in *Dirty Politics* that there was some connection between this attack and the leak. Technically, there is no obvious link between the two. A denial of service attack would not be expected to result in the disclosure of any information.

78. A denial of service attack is an attack designed to make a website unavailable to other viewers. It does this by bombarding a website with requests which keep the website too busy to respond to legitimate requests. It is the difference between protesters barring the entrance to a building and someone breaking into the building and rifling through the filing cabinets. It is possible that a denial of service can be used as a diversionary tactic while someone tries to access information. However, the best one can say for certain is that the two show an alignment of intent.

79. What the Police needed to do, including in their contact with Linode, is investigate the access that they knew had occurred to the data on www.whaloil.co.nz website. They failed to do this.

80. The Police were aware of all of these facts. **PD 7/1387** shows that they identified that an investigation of the host of that website might assist in revealing the leaker. It also shows that the Police telephoned Linode. The Police were informed by Linode that it did not hold any logs in relation to the denial of service attack. From the documents provided, this appears to be the full extent of the Police's investigation into www.whaleoil.co.nz. In my view this was wholly inadequate.

81. They should have sought a copy of the Virtual Private Server ("**VPS**") data on which the website was held. This would have given the Police a complete duplicate of all of the information contained in the system that was hosting the website, in a manner similar to the forensic cloning of Mr Slater and Mr Hager's computers for evidential purposes. **PD 7/1387** notes that Linode informed the police that this data was available from Mr Slater. However, there is no record of the Police following up on that information and seeking a copy of the data.

82. The VPS would contain logs about the access to its data, including the access that gave the Leaker the IP addresses that were shared with David Fisher and Nicky Hager. Those logs may well show whether the any of the weaknesses in the software that Mr Slater was using (discussed below) were exploited. In terms of an investigation into this crime, this is the main

place that the Police should have looked for that information. That the Police failed to obtain and do a thorough analysis of the VPS is the oversight that is most difficult to understand. It would have been at least as likely to show information that might reveal the Leaker as any other source of information.

83. There were also many more questions that the Police could have usefully put to Linode. In my view, they should have been put to Linode in any competent investigation.

84. For a start, the Police should have asked Linode for a list of all of the people who had access to the Linode customer account(s) for the VPS service that operated the www.whaleoil.co.nz website. This appears to at least include both Mr Slater and Mr [redacted]. The Police needed to know the complete list.

85. Next, the Police should have asked Linode for all of the logs for all access to the customer accounts relating to the VPS service for the relevant period including the IP address data for all of those accesses. If the Leaker had utilised access to the Linode customer account in the same way as with Facebook and Google, information about the source of this access may be present.

86. The Police should also have asked Linode for all of its customer service records in relation to these accounts. A common attack technique is to call the customer service centre for an online service provider and claim that you are the customer and that you have lost your password, and cannot use the regular password reset process. Customer service centres for many online services, including reputable services such as Apple and Amazon, have made the mistake of letting hackers into customer's accounts through such an attack. The Police do not appear from the documents to have undertaken any investigation into this possibility whatsoever.

The name registry and name hosting service

87. Another common technique for gaining unauthorised access to a website is to go through the name registry or name hosting service for the domain name. Again, the Police do not appear from the documents to have undertaken any investigation into these possibilities whatsoever. And again, these are enquiries that one might not think of if one does not have knowledge of computer crimes, but are amongst the most basic and obvious steps to take given that this was a computer crime.

88. The domain name is the text description of the website used to commonly identify it. In this case, it is "www.whaleoil.co.nz". When people type "www.whaleoil.co.nz" their computers needs a way of figuring out how to access that website based on that description. Equally, someone setting up a website needs a way of securing a domain name for their website that can reliably send people to the correct place. The way it works is essentially as follows.

89. Internet NZ is charged with managing all addresses that end with ".nz". Internet NZ, through a subsidiary called New Zealand Registry Services, authorises name registries to lease domain names to members of the public. When someone tries to register a domain name, the name registry will check that it is available. If it is, the name registry will agree a lease of the domain name for a set period. The person leasing the name will provide details of where the data for the website can be found. That information is given to a name hosting service for the website, often, but not necessarily, the same company as the name registry. The name registry will tell Internet NZ that the domain name has been leased, for how long, and the identity of the name hosting service.

90. When someone types "whaleoil.co.nz" into their browser their computer checks with a root domain name server which will tell it that, since it is a ".nz" site, they need to contact Internet NZ. When they contact Internet NZ, it will tell them the identity of the name hosting service. When they

contact the name hosting service, they will be told the location of the website itself – in this case that will be on the Linode servers.

91. There is an obvious potential avenue for compromising a website through this arrangement. If one is able to compromise a customer's account held with the name registry or the name hosting service then it is possible, for example, to change the information held by Internet NZ or held in the name hosting service, to misdirect traffic intended for the website. In particular, it would be possible to misdirect web browser connections or email connection. In theory, this could also be done by compromising Internet NZ itself, but this is a much harder proposition. This misdirected traffic can be intercepted and then redirected so that no one would necessarily know that they had been originally sent to the incorrect location. Intercepting the traffic would, for example, enable the interceptor to read passwords that were being typed into the website including the administrators' passwords.

92. In recent well-publicised examples, this technique was used to compromise the New York Times in August 2013, and Lenovo (a leading computer systems manufacturer) in February 2015. The people who compromised Linode in 2013 (referred to above) published an article on how they had done it. In this article they claimed that they had compromised Linode's registry in the way described above. However, they also found other security breaches, and it was these other security breaches that they used to obtain confidential information.

93. In order to investigate this possibility the Police needed to obtain information from Mr Slater about the name registry and name hosting service he was using. They then needed to obtain the logs for access to Mr Slater's accounts from those companies. There is no suggestion in the documents that have been provided that the Police took any such steps.

94. After a few minutes looking at public information of the internet, I was able to ascertain that whaleoil.co.nz was using a New Zealand company called FreeParking as its name registry, that the same company had been used as

the name hosting service before the denial of service attack, but that it changed to Cloud Flare after the denial of service attack. There is nothing in the documents to suggest that the Police even obtained this information or made any enquiries on the back of it.

Mr Slater's physical machines

95. As noted above, possible scenes of the crime include Mr Slater's physical personal computers and/or smart phones. The documents show that the Police considered this possibility. At **PD 7/1377**, there is a record showing that Mr Slater's personal computer was cloned. However, there is no record of any further investigation into that data. That data should have been examined for evidence of compromise. If there were any such steps taken, they have not been noted or the notes have not been disclosed.

People who claim to know who did it

96. I would have also expected the Police, at an early stage in their investigation, to speak to the people who were publicly claiming to know who the Leaker was. This perhaps should be at the top of the list of steps, but it is not an avenue of investigation I would necessarily expect to exist in every case of this type.

97. Mr Slater has publicly claimed to know the identity of the Leaker. The Police interviewed him. However, he is not the only one.

98. On 2 November 2014, Mr [redacted] mentioned above, posted an article on whaleoil.co.nz claiming to know the identity of the leaker. A true copy of that article is attached to this affidavit and is marked as Exhibit "**AJB-1**". As stated above, there is nothing in the documents provided to suggest that the Police made any contact with Mr [redacted] whatsoever.

99. It has also been very publically reported that John Key, the Prime Minister, knows the identity of the leaker. The public reports that I have seen about this date from late October 2014. A true copy of one such report is attached to this affidavit and is marked as Exhibit "**AJB-2**". This report dates from

after the search. Unless the Police were aware of this before the search, it is not a step that one can say should have been taken before doing the search. However, the Police confirmed in December 2014 that they have made no approach to the Prime Minister to see what information he holds. A copy of the letter setting out that information is at **PD 3/331**. The fact that they have now known about it for several months and seem uninterested in following up on it as a possible lead seems relevant. Particularly, it tests my theory that some steps were not taken by the Police because they were not competent in computer crime, and raises the possibility instead that the Police are making a deliberate choice to search Mr Hager rather than pursue other avenues.

Conclusion on other avenues open

100. There were therefore a large number of avenues of investigation open to the Police other than a search of Mr Hager's property, which were not explored by the Police. These avenues were things that anyone competent in computer crimes would have suggested. Some of them – for example talking to all insiders – are common sense steps that do not require any particular expertise. They were therefore steps that were known to the Police at the time of the search of Mr Hager's home, or ought to have been known to them if they had been acting reasonably and competently. These avenues of investigation included the most basic and obvious avenues that ought to have been investigated for a crime of this type, and the avenues most likely to bear fruit.

Chances of finding evidence

101. I am not able to comment on the chance that Mr Hager may have had at his house a piece of paper with "Rawshark = Joe Bloggs" or similar words written on it. That is not a question that falls within my expertise. As set out below, I know Mr Hager to be a person who is careful about protecting sources. I therefore personally consider such a thing to be very unlikely. My impression from reading the documents provided is also that the Police

had no expectation that finding a document of that kind was likely. However, that is a matter for the Court.

102. What I can comment on is the chance that a careful examination of Mr Hager's electronic equipment may reveal information that had been inadvertently left there and which would identify the Leaker. For the reasons that follow, and particularly based on what was publicly known about the Leaker and Mr Hager, I expect the chances of finding such information was extremely small. What is more, I believe from the documents provided that the Police knew that also.

The Leaker

103. As stated above the Leaker has publicly demonstrated a reasonable degree of competence in maintaining his anonymity.

104. Mr Slater's complaint records the fact that an attempt to gain access to one of his accounts was made from a TOR exit node.

105. TOR stands for The Onion Router. It is a system for obscuring the source of communication from the recipient. It can be used for other things, but that is its use in this context. It was originally developed by the US Naval Research Laboratory to facilitate the use of the internet for intelligence gathering without revealing the ties to the military.

106. To use TOR one must have a special piece of software. There is a community of people around the world who operate TOR relay nodes. The software creates a random path through these relay nodes from the origin to the destination. The data is then sent along this path in such a way that each node knows only the node before it and the node after it. Cryptographic techniques are used to ensure that this is the case.

107. A good analogy might be a letter that is sent by putting it inside a large series of nested envelopes with different addresses. Each time the letter is sent the person it is sent to opens one envelope and posts it again. That person will be able to see where it came from with the postage stamp, and

will be able to read where it is going to next. However, they will not know the rest of the chain.

108. The result is that the person at the other end of the communication chain from the person using the TOR software will not have any internet information that can reveal to them who is at the far end of the TOR communications chain.

109. Journalists who were communicating with the Leaker publically commented on the fact that the Leaker insisted on the journalists communicating through the use of "Tails". For example, Matt Nippert, who was at the time working for Fairfax, made this comment in a news story published on 24 August 2014 (**PD 5/872**). It seems a safe assumption that if the Leaker was insisting on journalists using Tails, he was using Tails himself. This assumption is also supported by Mr Slater's complaint which includes a picture of an email from Google, warning him of a suspicious attempt to access his account on 2 March 2014 from a system identified as a TOR exit node, suggesting that someone using TOR was attempting to break into his account.

110. Tails is a software package that includes TOR and some other anonymising software. The Tails programme makes it easy to use things like email over the TOR network. It also includes tools to prevent information from being left in the long-term memory of the computer that is running the software. The purpose of this is to defeat forensic analysis. Tails is effective in achieving this purpose.

111. The Leaker published cryptographic material on his twitter feed, @whaledump. This demonstrated that he was conversant with the use of cryptography.

112. Messrs Nippert and Fisher also publicly discussed the mechanisms that the Leaker had set up with them so that he was able to establish the authenticity of future communications. This again demonstrated an understanding of cryptography.

113. The Leaker sent tweets at highly regular intervals. This suggests that he had software that was pre-scheduling these tweets. This is a technique that people use so that the time of a tweet, or other form of communication, cannot be used as evidence to lead to that person's identification. The timing cannot be matched with the timing of the people's online activities. Also the person could go and set up a physical alibi for the time of the communications.

114. The Leaker also pre-loaded onto sites on the internet data that he intended to later leak. Once the leaks occurred, it became apparent that the data had been placed at those locations some days in advance. There was also an occasion when someone found data that the Leaker was going to leak before he had alerted the public to its existence. This again is a technique used to defeat an attempt to determine his identity through the timing of his known activities.

115. I also think that the Leaker's claim to be travelling to Vanuatu was the use of a technique known as chaffing. This was my immediate reaction when I first saw that tweet. I cannot be sure that this is the case. However, given the other steps that the Leaker took to hide his identity, the statement about going to Vanuatu seemed an obvious lie. Chaffing is analogous to the use of chaff by military aircraft. When the aircraft is targeted by a weapon it may release a cloud of material designed to fool the targeting system of the weapon and to obfuscate the aircraft's true location. Similarly, hackers sometimes deliberately drop false clues to their identity. Law enforcement are obliged to investigate those leads. This wastes the time of the law enforcement service. Enough "chaff" may make it unaffordable for law enforcement to explore every lead, and thereby uneconomic to investigate the offending.

116. Lastly, when the Leaker finished his public releases, before the search of Mr Hager's house, he said on twitter that he was destroying every device used in the operation and all of the encryption keys. I cannot say whether this actually took place. However, the fact that he said this means that he

was aware that this was a step that one ought to take to protect anonymity in circumstances such as these.

117. Together, these factors suggest that the Leaker was competent in the use of techniques to hide his identity.

Nicky Hager

118. Mr Hager and I have both presented papers at a conference together. It was at the New Zealand Centre for Investigative Journalism 2014 Annual Conference in June 2014. My paper was on digital operational security for journalists. In particular, I discussed the technical aspects of communicating with sources so as to protect anonymity. Mr Hager was the chair of the conference and attended my talk. Mr Hager also gave a presentation on developing and protecting sources, albeit not one that delved into technical aspects.

119. In general, I am aware that Mr Hager has an excellent reputation for protecting his sources.

The leaked documents

120. The Leaker has made at least some of the leaked material publically available. I have seen those documents. They appear to be the ones on which *Dirty Politics* is based in that they match Mr Hager's descriptions contained in *Dirty Politics* of the documents he was drawing from in writing that book. As far as I can tell, an examination of those publically distributed files does not reveal any information that might identify the Leaker. Assuming that those files are the same as the ones that Mr Hager had in his possession when writing *Dirty Politics*, it does not appear to be of any use to the Police to obtain those files. Indeed, I would expect that the Police already have those documents albeit they did not disclose copies of all such documents. All of those documents were made available before the general election, so well before the Police searched Mr Hager's house.

Police expectations

121. The Police were aware of the TOR/Tails issue set out above. They had Mr Slater's complaint and Mr Nippert's article. They had all of the Leaker's public comments. In addition, I have noticed a reference to Tails in relation to the briefing given before the search.

122. There is a printed copy of the briefing notes at **PD 8/1518-1523**. This makes no reference to any software issues. However, Detective Annalise Fergusson attended that briefing given on the morning of the search and took notes. These are at **PD 7/1390**.

123. Det Fergusson notes say "TAIL - software". This is the only reference to any software or indeed to any particular material that the Police were looking for or expected to find on Mr Hager's systems.

124. This all suggests to me that the Police fully expected that, like Messrs Nippert and Fisher, Mr Hager had been communicating with the Leaker using Tails.

125. As stated above, it is a core purpose of Tails to ensure that no inadvertent material is left on a computer. If, as appears to be the case, the Police expected to find Tails then they must have expected that it would be very unlikely that there would be any inadvertent material left on the computer.

126. I cannot say that finding such material is absolutely impossible. The Police could have believed that there might possibly have been such material. They might have gotten lucky. However, there is nothing in the documents that have been provided to me to suggest that the Police had any reasonable grounds to believe that they would find such material. And there is material to suggest that the Police knew that the chance of finding material was slim.

127. I note that these issues are not addressed in the application for a warrant at **PD 8/1459-1472**.

Conclusion on the chance of finding material

128. As stated above, I cannot say that it is impossible that Mr Hager had inadvertently left identifying information on his computer. There are certainly ways in which Mr Hager could have been sloppy in his practices and caused such information to be there. However, based on the material set out above, my view is it is very unlikely that they would find such material.

129. Mr Hager had the training to know what to do and what not to do. The Leaker had demonstrated competence in techniques needed to prevent such evidence being left.

130. The Leaker had demonstrated a consistent pattern of using Tails software and on insisting that others use Tails to communicate with him. The entire purpose of Tails is to prevent information being inadvertently left on the computer using it. Assuming only that Mr Hager had been following the same process as publicly disclosed by Messrs Fisher and Nippert, the chances of finding any evidence were very low. I think any computer security expert would express that same view.

131. I understand that the legal test will be whether the Police had reasonable grounds for believing that there would be evidence there. As I say, my considered view is that the chances of there being evidence are very low. It is also my view from the documents that the Police knew that. In any case, I have certainly seen nothing in the documents to suggest that the Police had a reasonable basis for considering otherwise – particularly if they were receiving advice from anyone competent in the field of computer security.

Affirmed in Wellington)
on the 2nd day of ~~April~~ April 2015)
before me)

C. A. McLachlan

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

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	

Affidavit of Nicolas Alfred Hager

Affirmed: 16 June 2015

Solicitor Counsel

Thomas Bennion
Bennion Law
L1, 181 Cuba Street
PO Box 25 433
Wellington 6146
Tel: +64 4 473 5755
Fax: +64 4 381 3276
tom@bennion.co.nz

Julian Miles QC
Richmond Chambers
L5, General Buildings
33 Shortland Street
PO Box 1008
Auckland 1140
Tel: + 64 9 600 5504
miles@richmondchambers.co.nz

Felix Geiringer
Terrace Chambers
No. 1 The Terrace
PO Box 10 201
Wellington 6143
Tel: +64 4 909 7297
Fax: +64 4 909 7298
felix.geiringer@terracechambers.co.nz

I, Nicolas Alfred Hager, investigative journalist of Wellington, solemnly and sincerely affirm:

Introduction

1. I am the applicant in these proceedings. I make this second affidavit in reply to evidence filed on behalf of the respondents.

Leaked information and information obtained from a crime

2. In his 1 May 2015 affidavit, Detective Inspector David Lynch tries to draw a distinction between leaked information and the source information for *Dirty Politics*. His arguments are based on a misunderstanding of something I said about the source information in *Dirty Politics*. He also lacks an understanding of how leaks and confidential sources work in the real world.

3. His argument begins in paragraph 21 where he says I had "acknowledged", in the Preface of the *Dirty Politics* that I had not used "this type of source before". He says he "took that to mean that the applicant had not previously received material that he knew had been obtained by a criminal act as opposed to someone who had legitimate possession of the material but chose to 'leak' it." In paragraph 24, he then presents this assumption about my meaning as fact, writing: "Given that the applicant accepts that he had not received material from a crime before, his analogies about how Police have dealt with him on prior occasions with material not obtained via a crime are not relevant as they compare two different situations."

4. DI Lynch was incorrect about my meaning. When I wrote that I had not used "this type of source before", I was referring specifically to information that I understood to have been obtained by hacking. I wrote about the type of source in order to be up front about the origins of the book.

5. Many of my confidential sources have risked criminal charges both because they were providing the information to me and because of the way in which

137

they gained access to that information. This is often an inherent part of whistle blowing and leaking, especially where very secretive, deceptive, unethical, or illegal activities are being investigated. It is particularly the case in my specialist areas of interest which involve military, intelligence, and secretive government activities.

6. DI Lynch continues in paragraph 60: "The applicant concedes that this case is unique in terms of the source of the information received. I am unaware of any other cases where a journalist in New Zealand has knowingly received material obtained from a crime which was used as the basis for writing a book." To find such books he need have looked no farther than my other books, as described in my first affidavit.

7. For instance, many intelligence and military sources gave me information and documents that formed the basis of my books *Secret Power* (1996) and *Other People's Wars* (2011). Many of these people risked charges under the Crimes Act in relation to both the way they obtained the information and the way they disclosed it.

8. In paragraph 66, DI Lynch concludes: "In my opinion the media/political commentators generally fail to accept that there is a distinction between 'leaked' information and information obtained from a crime." As explained above, my own experience of working with confidential sources does not support this distinction. In his reply affidavit, Mr Fisher cites the counter examples of Edward Snowden and Chelsea Manning. I am the main New Zealand journalist who has researched and written news stories based on both the Snowden and Manning documents.

9. As Mr Fisher explains in his reply affidavit, it is also not possible to draw a clear line between leaks where the leaker has obtained the document lawfully and unlawfully. In my 2012-2013 investigation of dodgy tax haven activities, for example, I did not know how the leaked tax haven records had been obtained.

10. In the case of *Dirty Politics*, I chose to be open about the fact that I understood the source to have obtained the material by accessing Mr Slater's computer system. However, I do not know the details about how this was done. I therefore do not know exactly how the criminal law may have applied to my source.

The chilling effect

11. In paragraph 66, DI Lynch uses his claims about the nature of leaking to argue that there could be no chilling effect on future sources from the raid on my home. He wrote: "the discussion of the so called 'chilling effect' is based on the premise that people who are in legitimate possession of information may no longer be prepared to pass on or 'leak' that information to journalists. That assessment is not valid in this case as the information did not come from a source of this nature, rather a person who has publically admitted obtaining the information by committing a crime."

12. This is incorrect in two ways. First, as discussed, his distinction between legitimate and criminal leakers does not match reality.

13. Secondly, even if he was right, the argument is illogical. If a person DI Lynch considered to be a "legitimate" leaker heard that the Police can arrive and conduct a broad search of all of my files and contacts looking for a particular confidential source then, whether or not that leaker may have themselves committed a crime in obtaining the material, he or she will naturally be much less likely to want to risk providing me with information. Some of my confidential informants' names would be immediately recognisable to the Police.

14. Even sources who have committed no crime in obtaining the information have almost certainly breached a rule of some kind in providing the information to me. They will not want to risk that being exposed. Even if they have done nothing wrong at all, they necessarily value their anonymity. If that were not the case then they would not be confidential

informants. They will therefore be deterred by the idea that the Police could possibly discover their identity in this way, even when looking for someone else. These people may have been prepared to expose wrongdoing and abuse of power and it is very important to society that they are not deterred.

15. I said in my first affidavit that I have already been contacted by confidential sources who are very worried about what the Police took. Likewise, the raid on our house, which was widely reported as the Police anticipated, cannot have gone unnoticed by possible future sources.

My public comments about the source

16. At paragraph 21 and 37, DI Lynch refers to the fact that I publically stated that I had received the leaked documents "out of the blue".

17. I, like other journalists, will usually say as little as possible about confidential sources. This was my attitude in drafting the preface of *Dirty Politics*. However, I wanted to be up front about my understanding that the material came from a hack and also make it clear that I had no knowledge of the material until after it had been obtained. I wrote that "I had no part in obtaining the material and I cannot say anything else about its origins"; and I had received the information "out of the blue".

18. The latter statement was intended to convey that until shortly before I received the information I had not known of its existence. However, I realise that that statement can also be taken to mean that I received the data without any prior discussion with the source. As explained in my first affidavit, that meaning would not accurately reflect what took place.

Paying the source

19. In paragraph 31, DI Lynch gives his reasons for seeking my bank account information. This includes a claim that he was looking for evidence of RawShark generating income from the book. The claim that this was what was being looked for was repeated by Crown counsel in an email of today's date (16 June 2015).

20. I have never paid money to a source in exchange for receiving information. Nor have I ever shared profits from a book or an article with a source. I cannot imagine circumstances where I would ever break this rule. Paying sources risks undermining the integrity of the information gathered. It is considered a no go zone by all but the most unethical journalists.

21. As I said in my first affidavit, I find it insulting that the Police thought I might be paying the source. I know of no basis upon which the Police might have believed that I was making any such payments. No information providing such a basis has been disclosed to me by the Police. For absolute clarity, no such payments were ever made to my source for *Dirty Politics*.

22. In fact, I went to great lengths to satisfy myself that my source was genuinely motivated by public interest. I did so in a variety of ways. I asked directly why they were providing material to me. I pressed the person about affiliations and possible political motivations. The source told me that their initial motivation was being upset about Cameron Slater's vicious attacks on people through his blog. Given the manner in which Mr Slater operated publically, my source had believed that Mr Slater's communications would disclose unethical activities. My source told me that their purpose in trying to obtain the information was to be able to expose it.

23. When we met, the source clearly cared about the implications of the material they had obtained. They pointed out the parts they believed were especially bad. The source was offended by many of the things they had

141

learned and believed that the public needed to know about them. I have had a great deal of experience dealing with confidential informants and attempting to ascertain their true motivations. I was convinced that this source was genuine in what they were saying.

Reasonableness of the belief there would be useful evidence in our home

24. In my first affidavit, I said that the Police had seized 104 compact disks and noted that "about ten of them contain very sensitive information given to me by a confidential source in 2003." In paragraph 68 of his affidavit, DI Lynch states that this comment "strengthen[ed] the view that we could reasonably believe evidential material" could be found about the identity of the *Dirty Politics* source by searching our home.

25. Obviously comments that I made in an affidavit several months after the raid are not capable of changing how reasonable the Police's belief was at the time they sought and executed the warrant. But, in any case, the inference is invalid.

26. As I explained in my first affidavit, I keep many files in our house in cases where I do not think there is a serious risk that someone may actively try to discover the identity of a confidential informant who gave me the information. It was completely different with the *Dirty Politics* materials. I would never keep any such information at home when there were a range of people, government and private, who were vigorously trying to discover the identity of the source. As I said publically, wrote in my first affidavit, and told the Police by phone after they arrived at our house, I did not have anything in the house that could help identify that source. For completeness, unlike the public statements I made in relation to the material on which *Dirty Politics* was based, I never claimed to have removed the documents from 2003 from our house. Nor in relation to any other documents have I claimed to have removed them from my possession when that was not in fact the case.

Consistency of police decisions compared to related cases

27. DI Lynch has suggested that the Police were obliged to search me in this way. At paragraph 12 of his affidavit, he stated:

> The allegation in this case carried a penalty of seven years imprisonment and commensurate with the level of offence, a case of this nature would generally have any obvious and practical lines of enquiry to identify a suspect pursued.

In paragraphs 40 and 41, he went on:

> Police would face in my view justified criticism for failing to follow all logical lines of enquiry in not executing a warrant on the applicant in this regard....
>
> Likewise in a situation where Police completed the investigation without executing the warrant and did not have sufficient evidence to charge an offender, Mr Slater would have grounds to complain to the Independent Police Conduct Authority about investigative failing. I would have to accept in that case that Police failed to follow an obvious and logical line of enquiry and could have been subject to criticism.

DI Lynch also denies any unequal treatment in his paragraph 62.

28. These comments have been questioned by former Police detective Wayne Stringer in his reply affidavit. Here, I question whether DI Lynch's statements are borne out when considering Police's decisions about investigating complaints against Cameron Slater and others whose actions are described in the book *Dirty Politics*.

Allegations in Dirty Politics

29. *Dirty Politics* set out several cases of possible criminal actions by Mr Slater and his associates. The Green Party laid a complaint with the Police after the book's publication concerning corrupt use of official information, blackmail, and unlawful access to the Labour Party's computer systems. The alleged unlawful access to the Labour Party computer system had been by Mr Slater himself and the Prime Minister's advisor Jason Ede.

30. Attached and marked as Exhibit "**NAH-3**" is a true copy of a December 2014 media report on the Police decisions in relation to the complaints. The report states that "Police have since reviewed the [first two] allegations and say they appear to fall short of criminal offending". Concerning unlawful access to the Labour Party computers, the Police were "still considering" the complaint and said that "if they do decide to investigate" it would be under a complaint from Labour, which was made that month. At that stage three months had already passed since the book's publication.

31. At the time of writing this supplementary affidavit, it is 10 months since the book was published. The Police have still not made any announcement about whether they are even investigating the complaint.

32. This approach contrasts with the tone of the investigation into Mr Slater's complaint about the source for *Dirty Politics*, and contradicts the reasoning in DI Lynch's affidavit. For instance, an email sent on Friday 12 September between two Police officers involved in the case states: "The attached production order is of importance to us and due to the sensitivity of the investigation, it would be greatly appreciated if this could be expedited for a turnaround on either Monday or Tuesday." The production order had been headed "urgent" and "high importance" (**PD 14/2362**).

Alleged computer crime against Matthew Blomfield

33. Similarly, the Police received another unlawful access to a computer system complaint against Mr Slater in 2012. The complaint came from a businessman named Matthew Blomfield, whose computer hard drive had

144

been stolen and given to Mr Slater by a disaffected former business partner of Mr Blomfield's. Mr Slater had searched through the hard drive and published a series of blog posts on the Whale Oil site accusing Mr Blomfield of a range of crimes, which have been the focus of a defamation case against Mr Slater since then. The facts in this case have been set out in the High Court judgment in *Slater v Blomfield* [2014] 3 NZLR 835. In that decision Asher J concluded that "the material provided by the sources appears to have been unlawfully obtained" (at [138]).

34. I have been following this case for some time and have had contact with Mr Blomfield. Mr Blomfield told me that he laid a complaint with the Police about the theft and unlawful access to his hard drive but that, some years later, the Police have still done almost no investigation and certainly have not raided Mr Slater's house.

Alleged procurement of hacking

35. In a third example, on 6 June 2015, TV3's *The Nation* programme broadcast a story alleging Cameron Slater offered money to a man named Ben Rachinger to hack into a left-wing blog site. The story included copies of text messages from Mr Slater arranging the hack and impatiently waiting for it to be completed. The programme revealed that Mr Rachinger had told the Police about the incident in February 2015.

36. The Police responded to the TV3 story confirming that they had "received a complaint regarding an alleged attempt to procure the hacking of a computer system". They said the complaint was being investigated by Counties Manukau CIB, the same office that executed the raid on our home, but said "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." By that date, it was about four months since Mr Rachinger had made the

complaint. Attached and marked as Exhibit "**NAH-4**" is a true copy of a NZ Herald report on this story including the Police comments.

37. In contrast, according to the Police documents released in discovery, the Police began work on the Slater complaint about my book before Slater had even made a formal statement and a month later judged it as "obvious and logical" to raid our home.

38. Each of these cases appears to contradict DI Lynch's claim that Police "follow all logical lines of enquiry", including executing warrants, to gather "sufficient evidence to charge an offender". The Police can be seen making judgements about whether and how urgently to investigate each of the alleged crimes by Mr Slater and in these cases there appears to be little urgency or priority being given to investigating him. This does not seem even handed.

The police approach to journalistic privilege

39. At paragraph 43 of his affidavit, DS Simon Beal says:

> We had considered the possibility that the applicant might claim journalistic privilege and how we would need to respond to any claim of that kind. I was aware that if he did so his claim to privilege would need to be determined by a High Court Judge and that we would not be able to access the documents in the interim.

In paragraph 44, he continues to explain that the Police prepared to seize and seal material on the day of the search. In paragraph 39, he makes it clear that the Police would have entered our home by force, but "only as a last resort".

40. DS Beal's evidence implies that issues of journalistic privilege during the search of our home would be dealt with by seizing and sealing evidence and leaving it for a judge to decide the privilege issues.

41. This position suggests that the Police can raid the home or office of a journalist such as myself without considering, in advance, whether journalistic privilege and the values it embodies might mean they were not entitled to do the raid at all.

42. The legal issues this presents are for the Court to determine. But from my position, as the person raided, this seems an inherently unjust process. The Police seized my business machines and papers, caused me thousands of dollars of cost, hundreds of hours of work, and months of disruption to my work, threatened the viability of my future work and livelihood, and caused upset to my family, all without considering whether any of this was lawful or justified. I do not accept that this is how the law is supposed to operate. I have not committed a crime. I was told by the Police that I am not a suspect. And yet, the Police have turned my life upside down and have delayed any issues about whether the raid should have taken place to be sorted out in Court later. By this point, much damage has already been done.

Affirmed at Wellington)
on the 16th day of June 2015)
before me)

N. Hager

A ~~Solicitor~~ Barrister of the High Court of New Zealand

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***

Second affidavit of David James Fisher

Affirmed: June 2015

This is the annexure marked _____

referred to in the within affidavit of

sworn at Auckland this 18th

day of June 2015.

Deputy Registrar, District Court, Auckland

Lorna Perkins
Deputy Registrar

Solicitor Counsel

Thomas Bennion
Bennion Law
L1, 181 Cuba Street
PO Box 25 433
Wellington 6146
Tel: +64 4 473 5755
Fax: +64 4 381 3276
tom@bennion.co.nz

Julian Miles QC
Richmond Chambers
L5, General Buildings
33 Shortland Street
PO Box 1008
Auckland 1140
Tel: + 64 9 600 5504
miles@richmondchambers.co.nz

Felix Geiringer
Terrace Chambers
No. 1 The Terrace
PO Box 10 201
Wellington 6143
Tel: +64 4 909 7297
Fax: +64 4 909 7298
felix.geiringer@terracechambers.co.nz

I, David James Fisher, journalist of Auckland, solemnly and sincerely affirm:

Introduction

1. I provided a previous affidavit in these proceedings affirmed on 27 March 2015. I have been asked to complete this further affidavit to reply to some affidavit evidence for the respondents.

Code of conduct

2. In my first affidavit, I affirmed that I had read the code of conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules. I continue to agree to comply with it in relation to this second affidavit.

Instructions

3. I have not provided a signed confidentiality undertaking in relation to the Police disclosure in this case. I have therefore not been provided with a copy of any of the Police disclosure documents. I have also not been provided with a complete copy of the Police affidavit evidence. I have been shown a draft copy of a reply affidavit from Mr Hager, and I have only been shown the extracts from the 1 May 2015 affidavit of Detective Inspector David Christopher Lynch and the 4 May 2015 affidavit of Simon Andrew Beal as they are set out in Mr Hager's affidavit.

4. I have been asked to comment on the opinions expressed by DI Lynch and DS Beal and the reply by Mr Hager to the extent that that falls within my expertise as set out in my first affidavit.

Is there a valid distinction between leaking and obtaining document by crime?

Police position

5. As Mr Hager notes, DI Lynch tries to draw a distinction between leaked information and the source information for *Dirty Politics*.

6. DI Lynch suggests, at paragraph 60, that *Dirty Politics* is unique in its use of documents obtained by a crime. DI Lynch then concludes, at paragraph 66, that the evidence in relation to the chilling effect is invalid because it fails to take account of this distinction.

7. In my view, the distinction that DI Lynch is attempting to draw is not valid.

The nature of leaking

8. Leaking is almost always someone doing the "wrong" thing for the right reasons. Providing the information to a journalist will almost always break some rule. It may not always be a crime, but it frequently can be. The crime could be in the act of leaking, but it could also be in the act of obtaining the information.

9. Most obviously, the obtaining of a document may frequently constitute theft. On one occasion, a confidential informant of mine took all of the contents of his manager's desk and delivered them to me. In doing so he was clearly stealing things that belonged to the company (part owned by his manager) and giving it to someone who would likely hurt the manager's interests.

10. That may be an extreme example. However, anyone who gives me a paper document could well be guilty of stealing the piece of paper on which it is printed. For example, this would likely be the case if they had obtained the copy by using the office photocopier.

11. Information is ubiquitously stored on computer systems. Informants who accessed documents on computers for the purpose of providing them to a journalist will know that they lacked the authority to do so and may therefore be committing a crime. There are crimes of copying some government documents. In relation to official information, it can also be a crime to leak it.

12. This is just one of the reasons why journalists have the obligations I discussed in my previous affidavit to ensure that they are acting in the public interest. It may be obvious that the theft of a piece of paper has occurred in providing me with some information. I need to ensure that the public interest in my using the information is sufficient to justify its use in those circumstances.

13. In the extreme example above, the manager's desk disclosed evidence of some serious criminal offending.

14. Many famous overseas leaking cases have resulted in criminal charges, or the threat of them, again relating both to the way they were obtained and disclosed. Daniel Ellsberg, who leaked the Pentagon Papers in 1971 that revealed the US government misleading the public about the Vietnam War, was charged with theft of government property and under the Espionage Act.

15. In recent times Edward Snowden came to prominence for leaking US and British intelligence documents showing unlawful, mass surveillance activities. In another case, Chelsea Manning (formerly Bradley Manning) famously leaked classified files starting with a video of US military personnel shooting civilians in Iraq. Snowden and Manning have both been charged with obtaining documents from crime (theft of government property) and charged under the Espionage Act for publicising them. Manning was also charged under the US Computer Fraud and Abuse Act.

16. These are just illustrative well known examples. In general, DI Lynch's distinction between proper leaks and information obtained from a crime is not consistent with the history of leaking.

17. I understand the reason for the protection of journalist sources is to protect the availability of information with a high public interest that is not accessible through other means. The need for such protection is for leakers who are breaking some law or rule by leaking. If a leaker is not "doing something wrong", it is very often not a real leak but just a backdoor release of information by people in positions of authority for their own ends. The need for journalistic privilege is to protect the ongoing availability of sources in the full knowledge that leakers frequently face the possibility of criminal charges. The role of the journalist - however the information was obtained - is to ensure that the source's motives for providing the information are not suspect and that the information itself is reliable and has sufficiently high public interest to justify its publication notwithstanding its source.

Not possible to draw a line

18. It is also not possible to draw a clear line, as DI Lynch appears to think one can, between leaks where the leaker has obtained the document lawfully and unlawfully.

19. First, in some cases, the journalist may not know whether or not a crime was committed. There is a spectrum of examples, including espionage and computer crimes, and through to possible charges of theft just because a leaker used the office photocopier. Sometimes it is not clear what the circumstances were because the journalist does not know the precise mechanism by which the information was obtained.

20. Secondly, when journalists do know whether or not a crime has been committed by their source in obtaining the information they may not set that out in their reporting. Journalists will usually say nothing about the source of their information so as to provide no information that might identify the confidential informant. The reader is therefore unable to tell if it was obtained in a way that constitutes a crime. Mr Hager's decision to comment on the source of the documents in *Dirty Politics* is an unusual exception to this rule.

Other examples involving hacks

21. However, *Dirty Politics* is not unique for being known to have been based on hacked materials. A very high profile example is the hacked material taken from Sony and released late last year. That has led to a large number of stories.

22. There are many other examples. Another high profile example involves the American politician, Hilary Clinton. She has been involved in two recent controversies. One concerned her role in relation to the attack on an American diplomatic compound in Benghazi, Libya. The other involved her use of a private email server for conducting State business. Both of these stories are said to have originating from a hack of an account belonging to her husband, former president Bill Clinton. Both stories were of enormous public interest in the United States. The revelations resulted

in Court action and a court order for the release of tens of thousands of pages of emails, including emails related to the Benghazi attack.

23. New Zealand had its own example of this when Foreign Minister Murray McCully's personal email was hacked, revealing that he had used his private email accounts. The report on this was in early 2012 claiming the hack had occurred in 2011. In doing so, he was circumventing the Official Information Act in a similar way to Hilary Clinton. The stories which followed revealed an unlawful pattern of handling information by a government minister which he has since pledged to correct. The content of the information was also reported. TV3 broke the story. To the best of my knowledge TV3 was not contacted by authorities. The New Zealand journalism community is small and I would have expected to have heard if any such contact had occurred.

24. A common type of story based on hacking is where the fact that the hacking was possible is itself the story. A hacker tells a journalist that they are able to access information that should not be accessible. The journalist then reports on this security flaw.

25. There was a high profile New Zealand example of this kind of a story in 2012. Blogger Keith Ng broke the story that it was possible to access large amounts of highly confidential information through WINZ self-service kiosks. In order to protect his source, Mr Ng initially suggested that he had found this flaw himself, but that source was later revealed. This was a major national news story of significant public importance. It led to urgent government reviews of information security.

26. Another example of possibly hacked information used for news purposes was the access by Cameron Slater of the Labour Party website. I was the first person to report on 12 June 2011. Mr Slater made contact with me in my capacity as a journalist for the Herald on Sunday, my employer at the time. He made contact because he said he wanted wider coverage of an exploit which had seen him take personal and confidential information from the Labour Party website. Mr Slater claimed that he had found unguarded open directories. The information as he accessed it was not

possible to be viewed or used in a coherent way, so he claimed that he had rebuilt it using software tools which were available. These events are discussed in *Dirty Politics* which gives a slightly different account to the one given to me by Mr Slater at the time.

27. The action taken by Mr Slater was widely reported as a "hack". It was information the Labour Party did not want made public and it required a level of technical proficiency to acquire it. Mr Slater, in contrast, said he had simply found access to the content of computers and used available software tools to rebuild the material so it could be used. Mr Slater had professed in the story I wrote there was no illegality in the access he had to the Labour Party website. A criminal complaint was made by the Labour Party to Police but as far as I am aware the Police say that they are yet to decide whether an investigation will take place.

Police themselves prioritise receiving information over some crimes

28. It appears that DI Lynch's intention in drawing this distinction between people who obtain the information in the course of a crime and other leakers is to suggest that the public interest in protecting the former is lower. However, I note that the Police themselves sometimes prioritise the public interest in receiving information above prosecuting crimes committed in the course of obtaining that information.

29. This is seen, for instance, in cases where a burglar decides to report something they have discovered in the course of a burglary. Attached and marked as "**DJF-2**" is a true copy of a media report of such a case in New Zealand. In that case the burglar reported finding a dead body. Given the burglar's decision to report this information in the public interest the Police in that case decided to take no action against the burglar. I am aware of similar cases in Spain and the UK, where the burglars reported finding child pornography, and in the United States of America, where a person broke into a car and found what they thought might be a terrorist's bomb.

Mr Hager's other sources

30. Lastly, I note that by attempting to draw this distinction DI Lynch clouds over a significant issue. The Police actions in this case do not just jeopardise the confidentiality of Mr Hager's source for *Dirty Politics*. By seeking to review Mr Hager's files they threaten the confidentiality of all of his sources. Indeed, I understand it to be Mr Hager's position that that source for *Dirty Politics* is in no jeopardy.

The police approach to journalistic privilege

31. DS Simon Beal adopts the position in his evidence at paragraphs 43 and 44, that issues of journalistic privilege would only arise if Mr Hager actively claimed the privilege and then, if he did claim it, that they would be dealt with by seizing and sealing evidence and leaving it for a judge to decide the privilege issues. I understand that this position is used to justify a claim that the Police can raid a journalist without considering, in advance, whether journalistic privilege might mean they were not entitled to do the raid at all.

32. I have seen Mr Hager's response to this proposition. His personal experiences in relation to this process are reflected in my own concern. The idea that the Police can come and seize a journalist's documents in this way without any prior consideration of whether such action is justified is a frightening thought. If implemented generally it could be expected to seriously impede the ability of the media to do their work.

33. Mr Hager is no less of a journalist than I or my colleagues at the NZ Herald. I do not understand how this rationale, if correct, would not also apply to our offices. I have already given evidence in my first affidavit describing how the Police have treated the organisations I work for differently, both before and after the introduction of the Search and Surveillance Act 2012.

34. My instinct is that the Police would have approached the NZ Herald in a completely different way, not the least because of the resources it could bring to bear to oppose such treatment. The wrongfulness of DS Beal's proposition would also be more obvious when it affects the country's leading newspaper rather than an independent journalist.

Affirmed at Auckland)
on the 18 day of June 2015)
before me)

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

Lorna Perkins
Deputy Registrar

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*

Affidavit of Wayne Leslie Stringer

Dated: ~~16~~ 22 June 2015

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

I, Wayne Leslie Stringer, retired police detective of Oamaru, swear:

Introduction

1. I have been asked to provide this affidavit to assist the Court on matters relevant to the judicial review brought by Nicolas Alfred Hager in relation to a warrant issued to the New Zealand Police to search Mr Hager's residence and examine his documents and computer systems.

Code of Conduct

2. I have read, and agree to comply with, the Code of Conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules.

Experience

3. I have worked for the New Zealand Police Service in various roles for a total of 32 years. Most recently, between 2001 and 2003, I was Area Controller for South Westland and Waitaki. Since then, I have been a Restorative Justice Programme Coordinator, a strategic advisor for the interim government of Bougainville, the Electoral Agent for then Cabinet Minister David Parker, and a mental health and Age Concern advocate.

4. Most of my time with the Police was spent in the Criminal Investigation Branch. I was involved in the execution of hundreds of search warrants. In most of these cases, I was one of the executing officers; in many, I made the application for the warrant; and in others, I supervised the process.

5. I have known the applicant, Nicky Hager, for some 20 years. I see him every few years and would describe him as a friend. However, we had no such discussions concerning the writing of his book *Dirty Politics*. I make this affidavit purely on the basis of my knowledge and experience of policing in New Zealand.

W.S.

This proceeding

6. I have been shown the application for the search warrant in relation to Mr Hager's premises. I have also been shown the affidavits of David Christopher Lynch, Simon Andrew Beal and Joseph Eng-Hoe Teo, filed in this proceeding. I have been asked to comment on several aspects of their evidence.

7. Most of my comments have a common theme. I am very surprised to see how much effort and police resource has been devoted to this case. The Counties-Manukau office routinely deals with large volumes of very serious crime, including murders, rapes, and crimes of violence and child abuse. Offenders in such cases, unless caught, have the potential to continue to cause extremely serious harm. Police have limited resources, and in my view rightly prioritise these crimes. In my view, the offence under investigation here, accessing a computer system for a dishonest purpose, is a much less serious offence than many others the police are called upon to investigate. Had I been in charge of the office, I would have accorded it a low priority. The amount of time and resource expended in this case seems to me to be akin to using a sledgehammer to crack a walnut.

The need for the search

8. In paragraph 14, DI Lynch says that "a case of this nature would generally have any obvious and practical lines of enquiry to identify a suspect pursued." I think this is manifestly untrue. In reality, the Police do not have the time and resources to follow all open lines of enquiry, even in relation to more serious crimes than this one. Many people who have been the victim of crimes such as burglary will be painfully aware of these limitations.

9. It is true that if there is a glaringly obvious line of enquiry in relation to an investigation of lesser seriousness (such as this one), police will often pursue that, if it can be managed quickly and is likely to get a result. But in my view, this is not such a case.

W.S

10. In particular, it does not seem to me that a search of Mr Hager's house was an obvious step in this case. On the police's account, Mr Hager was only a witness in this case. In all my years of policing, I have never executed a search warrant on the house of a witness. In fact, I have never heard of this happening. I am not saying it has never happened, but it must be very rare indeed.

11. Nor have I ever executed a search warrant over the premises of a journalist. These too were extremely rare. In my time on the force, Police knew such a proposed search required careful consideration.

12. In addition, careful consideration was always required when a warrant was to be exercised over a person's residence. Police have always accepted that these are very invasive and a strong justification is required.

13. In fact, in my experience, there are many cases where investigations into very serious offences were closed, even though there was a suspect and one possible line of inquiry would have been to apply for a search warrant over their houses.

14. For completeness, I note that the search of Mr Hager's house must have been very expensive for police. It involved five officers and a computer expert. Two had to be flown down from Counties-Manukau. Expense is always a factor in policing decisions.

Inevitability of search

15. For the same reasons, I am surprised to read that DI Lynch thought from the outset of the investigation that a search of Mr Hager's house was probable, and in fact was inevitable unless conclusive evidence of the offender's identity could be otherwise obtained (paragraph 39).

16. In my experience, such a decision depends on a range of factors, including the progress of the investigation, the requirements of other offences under investigation, the expense of a search, the likelihood of significant evidence being obtained, whether the search was at a home and (in this case) the fact

W.S.
160

that the target was not a suspect, was likely to claim privilege, and had reasonable grounds to fear the exposure of confidential sources who were not the subject of this investigation.

17. DI Lynch suggests that the police may come under "justified criticism" and even risk an adverse finding by Independent Police Conduct Authority if they failed to conduct this search (paragraphs 40 and 41). I cannot agree. I have worked on IPCA investigations. Although complaints are often made about investigative failings by the Police, I am not aware of any that have been upheld because police failed to execute a search warrant over the house of a witness. I cannot envisage such a complaint succeeding, in particular, where the target was not even a suspect.

Bank account information

18. In relation to the investigative steps the police did take, I see that DI Lynch says production orders were sought for Mr Hager's bank accounts. I understand from Mr Hager's lawyers that no such production orders have been disclosed, but that the evidence discloses that information requests were made to his bank. I understand that those information requests alleged that Mr Hager was under investigation for fraud. I see, from paragraph 31 of DI Lynch's affidavit, that these inquiries were made "to ascertain any travel movements that may have been able to be linked to the offender as well as assessing whether or not he was generating income from the proceeds of the book that could be considered proceeds of crime." I have been asked to comment on these matters.

19. I am puzzled by the reference to fraud by Mr Hager. I have considerable experience in fraud investigations as the Detective Sergeant in charge of company fraud in Wellington for several years. The police affidavits make no mention of any such suspected offending. They say they are investigating the offence of accessing a computer system for a dishonest purpose. I do not understand why they were invoking fraud by Mr Hager as a reason to receive information from the banks.

W.S.

20. In any event, this allegation of fraud that the Police used to obtain the bank information is not the same reason given by DI Lynch for obtaining the information in his evidence. He talks of travel information and proceeds of crime.

21. In relation to the travel information, I am surprised that Police would seek bank information for this purpose. For one thing, it would be unlikely to disclose any destination. For another, even if it did lead to the discovery of a destination, that would be unlikely to provide much assistance to the investigation as it would not reveal the purpose of travel or any location more specific than a city. For another, an attempt to track all the travel of someone like Mr Hager would be an enormous and probably fruitless endeavour.

22. In relation to the proceeds of crime, this also strikes me as odd. I would have expected that before taking such a step the Police would have had some evidence that suggested that Mr Hager had been paying for or had been paid for a crime. In my view these are very tenuous justifications for the use Police powers to attempt to search bank records.

The decision to apply for the warrant

23. I am somewhat confused about who made the decision to apply for the warrant. I would expect this to be very straightforward: the decision was DS Beal's to make as the officer in charge of the investigation. His affidavit suggests that this is the case, and that DI Lynch merely "approved" his decision (paragraph 21). However, DI Lynch says that he made the decision (paragraph 43). DI Lynch later says his decision to execute the warrant was "approved" by Assistant Commissioner Burgess (paragraph 53).

The contents of the warrant application

24. I have been asked to comment about the contents of the application for the warrant in this case. My view is that the grounds for the warrant are very thin and speculative. The reasons given are nebulous. They rely, in part, on

WS.
162

the assumption that Mr Hager lied about returning his source's material, and that he would be sloppy about protecting his source. I do not believe that application contains sufficient grounds for a reasonable belief that useful evidence would be found at Mr Hager's house.

25. In my view the application can also be criticised for what it omits. Police are well aware that they need to include all information relevant to the application, even if it does not assist their request. I would have expected Police to mention, at a minimum, the fact that Mr Hager was a journalist, the legislative protection given to journalists in the Evidence Act, and the fact that they were aware that Mr Hager could well have a basis for claiming that privilege. Given that this is not a common issue in relation to warrant applications, I would have been inclined to also set out previous relevant case law relating to searches concerning the media and the requirements that that imposed. They did not. That is particularly surprising to me, given that they say they took legal advice. I would also have expected them to provide more detail over the other steps in their inquiry that they had not yet completed. They admit that there were such incomplete enquiries. The details was needed so that the judge could decide whether a search of Mr Hager's home was warranted at that stage.

Execution of the warrant

26. I am familiar with the claims made by Mr Hager in his statement of claim about the breaches of privilege that occurred during and after the search. I have read the responses contained in the three police affidavits I have mentioned.

27. I was very concerned to see that, in several instances, the Police conducting the search and Police off-site used information from that search to advance their investigation. It seems they did so after privilege had been invoked. In my experience, Police understand full well when they are crossing the line between securing material and searching it. They must have known that what they were doing was wrong when they used the contents of material

W.S.
163

that they were only permitted to secure, in order to derive some benefit for their investigation. In my view that certainly seems to be the case, at the very least, in relation to the use of information derived from Mr Hager's mobile phone IMEI number and SIM card number after the search was over; the information in an email that Detective Teo recorded on a job sheet nearly three weeks after the search (which would then have been accessible on the investigation file); and the photographing and emailing of information to the National Cyber Crime Centre during the search. There is nothing in the reasons given in the police affidavits that alters my view that it would have been obvious to Police that they were going beyond simply securing information, and moving into the zone of searching it.

28. The Police evidence attempts to justify these breaches by saying that there was an urgent need for them to act (for example Beal at paragraph 58). However, any police officer would know that this is not their decision to make. If they need to conduct urgent enquiries based on the seized information where privilege has been asserted then they should have made an urgent application to the Court for permission to do so explaining their reasons for saying that urgent actions was needed.

29. I have been asked to comment on anything else I thought was notable about the way the search was executed. I make three points. First, I am surprised that the Police did not wait until Mr Hager was home before conducting the search. In my view, it would have been easy for them to tell when he was there. Instead, they prepared for the possibility that he would not be there and were prepared to break in if necessary (Beal affidavit, paragraph 39). This would have denied Mr Hager any chance to invoke privilege, as Police must have known. This seems wrong to me, particularly given that Mr Hager was not a suspect.

30. Second, Police began conducting their search before they gave Mr Hager an opportunity to invoke privilege. DS Beal's evidence is that he only gave Mr Hager an opportunity to invoke privilege in his second phone call with him.

W.S.

I understand from Mr Hager's lawyers that the phone contact only came about because Mr Hager's daughter called him, not because of an effort on the part of the Police to contact him. At any point during the search, officers may have come across and read material that exposed confidential sources, whether or not they were even relevant to the investigation. Police must have known that. Again, this seems wrong to me.

31. Finally, Mr Hager's lawyers told me that Police bore hidden recording devices throughout the search. I have never heard of this happening before. It seems particularly extraordinary in that Mr Hager was being treated as a witness.

Sworn at ~~Wellington~~ Omaru)
on the ~~16th~~ 22nd day of June 2015)
before me)

WISTRINGER.

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

P J. Bond, JP
#13105
OMARU
Peace for New Zealand

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***

Second affidavit of Adam Julian Boileau

Affirmed: 16 June 2015

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

I, Adam Julian Boileau, computer security consultant of Wellington, solemnly and sincerely affirm:

Introduction

1. I provided a previous affidavit in these proceedings affirmed on 2 April 2015. I have been asked to complete this further affidavit to address matters arising from documents provided by the Police since the completion of my first affidavit and to respond to the affidavit evidence of the Police witnesses.

Code of conduct

2. In my first affidavit, I affirmed that I had read the code of conduct for expert witnesses set out in Schedule 4 of the New Zealand High Court Rules. I continue to agree to comply with it in relation to this further affidavit.

Instructions

3. Since completing my affidavit I have been provided with further discovery provided by the Police. I understand that these documents have been included in four further bundles of Police Disclosure volumes 11-14 exhibited in affidavits from Linda Cheesman.

4. I have been asked to review these documents and to comment on whether they affect the opinions set out in my first affidavit in any way.

5. I have also been provided with the following affidavits to review:

    5.1. Ian Stephen Donovan affirmed 30 April 2015;

    5.2. Brent Peter Whale sworn 1 May 2015;

    5.3. David Christopher Lynch sworn 1 May 2015;

    5.4. Joseph Eng-Hoe Teo sworn 1 May 2015;

    5.5. Simon Andrew Beal sworn 5 May 2015;

    5.6. Rex Arthur Cottingham sworn 5 May 2015;

D

167

5.7. Simon Andrew Beal sworn 22 May 2015; and

5.8. Joseph Eng-Hoe Teo sworn 2 June 2015.

6. I was asked to comment on the evidence set out in those affidavits to the extent that they fell within the scope of my first affidavit and within my area of expertise.

Overall impression

7. The new documents do not alter my previous opinions. Several new documents provide more support for those opinions.

8. The new documents provide a more complete record of what technical investigations took place. They included, for example, the job sheet of the person charged with leading the technical investigations (**PD 11/2116**). The last viewable entry in that jobsheet is from 18 September 2015. I am instructed that there were an additional 11 pages of that jobsheet after the one shown on **PD 11/2123**, but that all text on those pages was redacted.

9. There are a couple of minor steps that were taken of which I was not previously aware. However, these do not include any of the steps that I suggested should have been taken in my first affidavit. The fact of those other steps merely reinforces my view that the people conducting this investigation were wrongly treating it as a crime involving computers rather than a computer crime.

10. I make reference to some of the new documents below. However, the information contained in those new documents has been overtaken to some extent by the evidence that has now been filed. The evidence sets out the Police narrative of what investigations were conducted. I have therefore concentrated on replying directly to that evidence.

11. Again, the evidence confirms my understanding of what took place (and did not take place) from the previous documents. It therefore reinforces my view from the first affidavit that avenues of investigation were open to the Police other than a search of Mr Hager's property, which were not

explored by the Police. These avenues included the most basic and obvious avenues that ought to have been investigated for a crime of this type, and the avenues most likely to bear fruit.

12. With respect to most of these avenues of investigation, the Police evidence either fails to address them or acknowledges that they were possible and offers no valid explanation as to why they were not pursued.

13. The Police evidence also fails to offer a valid explanation as to why the Police had reasonable grounds to believe that they would obtain evidence from a search of Mr Hager. Indeed, the expert evidence offered to respond to my own, from Mr Whale, does not go higher than to claim that it was possible that the Police would find such evidence.

Simon Andrew Beal

Supplementary affidavit of 22 May 2015

14. On 22 May 2015, DS Beal gave a supplementary affidavit correcting paragraph 12 of his previous affidavit. He had previously suggested that a forensic examination of Mr Slater's computer had been completed by the time he executed the warrant (with the report of the analysis being completed later). He corrected this to claim that he had been told that:

> By the time of execution of the search warrant, I had been informed verbally that i-mac computers were highly resistant to malware and compromises and that it was therefore highly unlikely that anything of value to the investigation would be found.

15. There are many problems with this statement. The statement is further evidence that suggests that the people running the technical aspects of this investigation did not know what they were doing.

16. Malware is short for malicious software. Typical malware is mass-market, designed to be used on a large, indiscriminate set of victims. Some malware, such as the stereotypical computer virus, is propagated through automated systems, where the author cares little for specific victims.

17. Like any software, malware will be engineered for a particular computer platform. There have historically been many more Windows computer systems in operation than Apple or others. Windows and its predecessor DOS have many more catalogued malware samples because of this historical market share during the period where viruses and malware became prevalent.

18. In present day malware, there is no meaningful difference between modern Windows and Apple computer platforms. Both platforms are generally robust, but experience periodic technical flaws and user behaviour which can lead to compromise by malware or other agents.

19. Any such distinction between Apple and Windows computer systems is, in any case, irrelevant. It seems certain that this case did not involve automatically distributed or mass-market malware. The strong suggestion is that it was a targeted attack against Mr Slater.

20. Typical malware will use degree of autonomy either because it is entirely self-contained, as in the case of a virus, or because the number of targeted systems is beyond the capability of the attacker to manage by hand, as with financial crime malware that attacks internet bank customers. A targeted attacker does not need the added complexity of such automation. They have the necessary time to carry out the activity by hand.

21. Targeted attackers do not, contrary to what a layperson may have "learned" from the movies or television, need to use viruses or malware. Modern computers are designed to interact with a network, and contain sufficient features and tools whose legitimate functionality can be co-opted to carry out the tasks of hacking.

22. A targeted attack on Mr Slater's computer is likely to leave forensic artefacts, some types of which are described by Mr Whale's affidavit. These artefacts are not likely to be those of malware or viruses. The historical prevalence of malware on non-Apple computer platforms is of no relevance in concluding the likelihood of the presence of such evidence on

Mr Slater's computer. If someone told DS Beal that this was relevant, then that suggests to me that they had a fundamental misunderstanding of the nature of the computer crime that they were investigating.

23. In addition, before concluding their analysis of Mr Slater's computer there is no way the investigators could have known that it would not be a fruitful investigation.

24. The documents with which I have been provided do not include any report of what analysis was done of Mr Slater's computer. I am therefore unable to comment on whether Mr Slater's computer was analysed appropriately. However, DS Beal's statement gives me reason to think that the people conducting the analysis were looking for the wrong things. It suggests that they were analysing the computer for automated malware. Such an analysis would not be expected to reveal the things for which they ought to have been looking.

25. The analysis should have been looking for evidence of targeted computer intrusion, such as (by way of example): suspicious emails, suspicious chat messages or other communication, suspicious web browser history, or other technical artefacts from the type of hacker techniques used by a human attacker. They should not have been looking only for automated malware or viruses. They also could not be expected to find the things they should have been looking for inadvertently while conducting a search for automated malware or viruses.

26. Since doing a first draft of this reply, I have been provided with yet further discovery documents provided by the Police. Some of these documents further strengthen my view as set out above.

27. On 17 September 2014, DS Beal wrote an email in which he noted that there was no one in the Electronic Crime Laboratory in Auckland with the capability of doing the necessary analysis of Mr Slater's computer (**PD 13/2202**).

171

28. On 18 September 2014, DS Beal writes an email in which he notes that "locating potential malware on a mac is a first for ECL I believe" (**PD 13/2206**). Later that day, Matt Taylor replies saying "I was going to bring this up at Monday's management meeting and discuss who in our group would be best placed to review the Mac for malware/virus compromise, but I see Simon has beaten me to the punch" (**PD 13/2205**).

29. On 16 September 2014, two of the officers working in this investigations team exchange emails with the subject "Op Oracle" (**PD 14/2256**). They appear to be seeking advice in relation to this case from a person whose name has been redacted and has apparently described themselves as knowing "the basics about cyber crime and hacking".

30. These exchanges confirm my view that they were looking for the wrong things on Mr Slater's computer. It also suggests that I may be correct in my view that the problem was that they lacked someone with the necessary expertise.

Paragraph 14

31. As noted below in relation to Det Teo's evidence below, it is my view that DS Beal is wrong to assert at paragraph 14 that all relevant files and logs in regard to the website had been deleted. Det Teo's evidence is that much of the website data had been preserved. The Police have wrongly concluded that that data is not relevant to their enquiries.

32. Secondly, DS Beal says that getting a list of users was no longer pertinent because the logs were no longer available. Even if the logs were no longer available, it is wrong to say that the user list is not relevant. The lists of privileged users (those with sufficient access rights to the misappropriated data) would give the Police a list of people with the means to carry out this intrusion. It was a list of possible suspects and certainly a list of people to whom the Police should have spoken. If the intrusion was not done by one of these people then it could have been by someone they knew who gained access to one of their access credentials.

Paragraph 30

33. Despite his supplementary affidavit of 22 May 2015, DS Beal has not amended his statement at paragraph 30 of his first affidavit. In that paragraph, DS Beal claimed that the lines of inquiry had either reached an end or "could not be completed for an extended period of time". DI Lynch says something similar at his paragraph 32.

34. In his supplementary affidavit, DS Beal says that he received an update after the search of Mr Hager's residence saying that the analysis of Mr Slater's computer had not found anything of evidential value. He does not say when he received that update.

35. I have been asked to opine on how long such an analysis would be expected to take. This is a "how long is a piece of string" question. I cannot say precisely how long it would take in the absence of the system. It also depends to some extent on how much resource the Police wished to expend and therefore how thorough a search they wished to conduct. However, I would say that it would take in the order of a low number of weeks and certainly not several months. The Police had had Mr Slater's computer for two weeks by the time of the application for the search warrant. I am of the view that the fact that the Police were awaiting the outcome of this analysis is not consistent with DS Beal's claim that the continuing lines of enquiry could not be completed for an extended period.

36. Below I address the accuracy of these statements in relation to other possible lines of enquiry that were still open to the Police.

David Christopher Lynch

Paragraph 8

37. It is not within my expertise to comment on which branch of the New Zealand Police should have conducted this investigation. However, it is worth noting a false assumption that is recorded in paragraph 8 of DI Lynch's affidavit.

38. DI Lynch says that "the location of Mr Slater's computers when they were 'hacked' was within the Counties-Manukau Police District". The computers that were hacked, if indeed that is an accurate description of what took place, were almost certainly the servers of a company located outside of New Zealand. This is not just my opinion, it was also the assertion of Mr Slater when he filed his original complaint as discussed in my previous affidavit.

39. Documents in the late discovery show that at least some of the Police shared my view that one cannot assume that a hack had even occurred. On 5 September 2015, Rex Cottingham, the "go to" technical investigator for the investigation (**PD 11/2048**), sent an email to DS Beal (**PD 11/2046**). He recorded a news report of the Leaker's online comments that suggested the Leaker had "acknowledged he could go to jail for hacking the WhaleOil blog". Mr Cottingham asked "Is that statement correct, that whaleoil.co.nz was unlawfully accessed". Later that day, DS Beal responded saying, "We are not 100% sure of the nature and extent of the compromises yet. That is part of the allegation."

40. As all of the Police evidence acknowledges, the avenues of investigation that have been completed have all been dead ends. The Police are no further along in determining what took place than they were on 5 September 2014.

41. In my view, DS Beal's position as per his email of 5 September 2015 was correct. It is wrong to assume that there has been a hack, as opposed, for example, to a leak by someone with some degree of authorisation to access the material but no authority to disclose it. In the absence of any information since that time, this should still be the position.

Paragraph 26

42. At paragraph 26, DI Lynch says the police conducted a review looking for people who would have the ability to conduct "the kind of hacking that was done here". I can see three problems with this statement.

43. First, the Police evidence suggests that this possible line of enquiry was raised but in fact it was not pursued (affidavit of Rex Cottingham at paragraph 12).

44. Secondly, the documents that have been provided suggest that the Police have made no progress on determining what kind of hack was done here, or indeed whether any hacking was done here. In the absence of knowing anything about how Mr Slater's data was compromised, it is simply absurd to try to compile a list of all people who had the skills to do it.

45. Thirdly, even if the Police did know exactly what had occurred in this case it is still absurd to try to draw up a list of everyone capable of doing it. This list would be enormous. There is also no reason to believe that most people with such capabilities would be able to be identified from "open source material".

46. A much more sensible approach would be to try to draw up a list of people known to Mr Slater who had such capabilities. Indeed, this is a point I raised in my first affidavit and the same point was made by Rex Cottingham (at his paragraph 12). However, as best as we can tell from the documents provided, this much more sensible route was never pursued.

Paragraph 32

47. At paragraph 32, DI Lynch states that:

> By 29 September 2014, some of our lines of inquiry had reached an end. Others were ongoing but were likely some months away from providing us with any information.

48. I have discussed this paragraph above in relation to DS Beal's paragraph 30. As stated above, I do not think this statement is consistent with the fact now revealed, that the analysis of Mr Slater's computer was not complete at that time. I also express below my doubt that this statement is consistent with other information about avenues of investigation that the Police knew about but were not pursuing.

Paragraph 37

49. [redacted]

50. First, I note that Mr Hager had publically said that he had not retained this flashdrive. This is noted in the warrant application (eg at **PD 1/29**). To believe that the search would recover the flashdrive during the search, the Police had to believe that Mr Hager was lying.

51. The warrant application states that the Police believe that Mr Hager had retained "material used to write the 'Dirty Politics' book to show provenance should there be future litigation against him" (**PD 8/1471**). I understand this to mean that the Police believed he would have retained the leaked documents in case someone suggested that Mr Hager had been making stuff up. Even if this is correct, it does not follow that Mr Hager had retained the original storage medium. It is this original flashdrive that is required for such forensic analysis. Merely having a copy of the documents is insufficient. This is clear because the Police had a copy of the documents. They were made publically accessible by the Leaker and, as stated in my first affidavit, I have myself looked at the same copies of the documents.

52. Secondly, even if Mr Hager was lying and the Police managed to retrieve the original flashdrive, I believe that a forensic analysis of that flashdrive was very unlikely to produce anything of evidential value. My view is based on the fact, as discussed in my first affidavit, that we know the Leaker was familiar with Tails. Tails includes tools that would enable the Leaker to transmit documents on a flashdrive without leaving any forensic information of evidential value.

53. This is not an obscure use of Tails known only to expert users. There is a step by step guide in the official Tails documentation that describes exactly how to do this.

54. Further, as discussed in my first affidavit, someone in the position of the Leaker is most likely to inadvertently leave a forensic trail when taking steps before they are conscious that they are doing criminal acts that are likely to be investigated. They are relatively unlikely to do so once they are conscious of the jeopardy they are in. The Leaker's provision of documents to Mr Hager must logically have occurred after he obtained those documents from Mr Slater. Everything we have seen about the Leaker since that time suggests that he has been very conscious of his jeopardy and has been taking steps to protect his anonymity.

55. Combined with the knowledge of the Leaker's competence in relation to hiding his identity demonstrated through other parts of the investigation, this leads me to the conclusion that the probability of obtaining useful information from such a forensic analysis was very low.

56. Thirdly, I note that after the release of *Dirty Politics*, the Prime Minister did in fact accuse Mr Hager of making stuff up and challenged him to release the documents. For example, Mr Hager is interviewed about this on television (**PD 1/67-68**). Mr Hager's response was that he cannot release the documents because he no longer has them. He also says that he asked for the documents from the Leaker so that he could release them and the Leaker refused. Mr Hager suggests that the refusal was on the basis that the Leaker was going to release the documents himself. The Leaker then did release the documents. All of this had happened, and was known to the Police, before they applied for the search warrant. This appears to be wholly inconsistent with the Police justification for saying that they believed Mr Hager had retained the flashdrive.

57. I cannot say that it was impossible that both Mr Hager and the Leaker were careless and that such evidence could have been found. But while this is a

177

possibility, the information available to the Police at the time suggested that it was very unlikely.

Paragraphs 71-74

58. At paragraphs 71-74, DI Lynch criticises my references to Mr [redacted] and the Prime Minister stating that they knew the identity of the Leaker. He points out that both statements postdate the search. This is right. However, in relation to Mr [redacted] I do not think that DI Lynch's criticism is valid.

59. My point in my first affidavit in relation to Mr [redacted] was that he was someone who could well have had access to Mr Slater's computer system sufficient to enable him to more easily leak the material than an outsider. This made him someone who the Police ought to have spoken to at the outset of their investigation. If they had spoken to him, then one would hope that Mr [redacted] would have passed on his knowledge about the identity of the Leaker. It appears from the documentation that the Police have never spoken to Mr [redacted]

60. DI Lynch says that Mr [redacted] information is joint knowledge that he shared with Mr Slater, and which Mr Slater has shared with the Police. How could the Police know this when they have not spoken to Mr [redacted] This appears to be a simple, quick, and resource light step, that could and should have been taken.

61. This also does not answer the question about why Mr [redacted] is not being investigated as the possible culprit.

62. At paragraph 74, DI Lynch justifies not investigating [redacted] not to mention the many other possible insiders (or even taking steps to list all the insiders with access), by saying that the Leaker has publically admitted that he has committed a crime for which he can face 7 years in jail. I can see four problems with this statement.

63. First, this is an example of a number of places in his evidence where DI Lynch appears to rely on the veracity of statements made by the Leaker

178

to support his reasoning. As stated in my first affidavit, it is common for people in the position of the Leaker to misdirect potential investigators. I said that I thought the reference to a trip to Vanuatu was such a misdirection. However, it may be worth noting that there were several other clear examples of such misdirection (see, for example, **PD 5/860,** where most of these are discussed):

63.1. the Leaker's Twitter account listed his address as being 3 Hans Cres - the address of the Ecuadorian embassy in London where WikiLeaks founder Julian Assange is exiled;

63.2. the Leaker's Twitter account also included an encryption key which resolves to Winston Peters' email address;

63.3. the Leaker distributed some information through a link hosted on the encrypted Mega website set up by Kim Dotcom; and

63.4. [redacted]

64. I regard it as a rule for investigating a crime of this type never to take at face value anything that is being said by the suspected intruder. It is therefore difficult to understand why Lynch is so ready to rely on the public statements of the Leaker.

65. Secondly, I am not a legal expert and I will have to rely on the submission of counsel. However, as someone who practises in the area of computer crime, I am unaware of any reason why someone in the position of Mr [redacted] would not also be liable for the same crime as an outside hacker were he to have abused his access for a dishonest purpose. I therefore cannot see why he would be any more or less likely to make such a statement.

66. Thirdly, in my experience, people operating in this field are generally not legal experts. While there are common understandings in very general

179

terms about what might be legal or not legal, I would not rely on the Leaker to correctly understand his or her legal liabilities for what has occurred.

67. Fourthly, DI Lynch's justification seems at odds with the contemporaneously expressed views of DS Beal. DI Lynch is using this statement from the Leaker to justify his investigation team taking no action in relation to insiders. However, as noted above, the officer in charge of the investigation, DS Beal, is recorded as expressing the view on 5 September 2014 that the same statement by the Leaker could not be relied upon (**PD 11/2046**). DS Beal's position appears to suggest that the statement by the Leaker cannot be the reason why the investigation team failed to investigate insiders.

68. In relation to the Prime Minister, I acknowledged in my first affidavit that this revelation came after the search and was not relevant to the question of what the Police knew at that time. That is not the point.

69. The point is that the Prime Minister, the most senior government official in the country, has publically said that he knows the identity of the Leaker. And yet, come December 2014, the Police had still not spoken with him. I gather from DI Lynch's affidavit (although this is not expressly stated) that the Police have still not spoken to the PM. He certainly does not say that they have, and I would have expected him to say so in answer to this point if that had now been done. While this does not directly affect the assessment of what the Police could have done at the time of the search, it does raise doubts about the good faith with which the Police are conducting the inquiry as a whole.

Brent Peter Whale

70. In paragraph 25, Mr Whale lists some steps that were taken to identify the Leaker. He states in paragraph 26, that these show that the Police investigation was not narrowly focused.

71. Mr Whale lists seven steps. These steps really represent two lines of inquiry. One seeks IP addresses related to the access of some of the leaked

information (Google, Facebook, Orcon and Yahoo) and the other seeks IP addresses in relation to the distribution of the information to the public (Wikisend and Twitter). Mr Whale asserts that these lines of inquiry had potentially good outcomes. As stated in my previous affidavit, there were many more, better, lines of inquiry.

72. I note also that the Police did not actually complete some of the lines of inquiry that Mr Whale identified. Det Teo makes clear:

72.1. at his paragraph 14, that Twitter required the Police to make a Mutual Assistance request, and the Police chose not to do so; and

72.2. at his paragraph 15, that Google required a US court order to release some of the requested information and the Police do not appear to have done so.

73. The same thing happened when (at paragraph 20 of Det Teo) Vodafone and (at paragraph 22 of Det Teo) TradeMe required production orders.

74. Mr Whale, at paragraphs 28-30, suggests that my one of my suggested avenues of investigation had a low chance of success. His reason was that the Leaker would have the ability to mask their true IP address and hence their location. The problem with this criticism of my evidence is that it applies with more force to the steps that were taken by the Police which Mr Whale praises earlier in his evidence.

75. Indeed, the results of the steps that the Police did complete were that the IP addresses had been masked and could not be used to identify the Leaker. As stated in my first affidavit, this was always going to be the more likely outcome in relation to these steps. That is because these steps certainly, or almost certainly, occurred after the Leaker was conscious of his jeopardy.

76. Again, as previously stated, the best hope in these circumstances is to trace the intrusion back to an early point where the Leaker was not yet aware of his jeopardy and was therefore not masking his location. The steps that I

suggested, for the reasons previously given, were more likely to be targeting those early acts of the Leaker.

77. Mr Whale's conclusion in paragraph 30 was that the chance of identifying the Leaker by examining the Virtual Private Server ("**VPS**") was low. I would accept that it was low given the lack of information about what occurred in this case. However, the chance must logically be higher than the chance of identifying the Leaker through all of the steps that were taken. Those other steps had at least all of the same difficulties.

78. At paragraph 31, Mr Whale dismisses my suggestion that the Police should have investigated the registry and hosting services. He accepts that these techniques are used to obtain unauthorised access to websites. He says that there is nothing to suggest that this was the method used in this case. However, there is nothing to suggest that any method was used in this case. The Police are completely in the dark as to how the attack happened. They only know that the data in the website was compromised. The steps I suggested were obvious steps to pursue given this lack of knowledge.

79. Mr Whale is silent on the steps that I suggested in respect of Linode other than the VPS. Like Det Teo (as discussed below), I suspect that he is wrongly conflating those steps with the issue of the VPS. As stated below, those steps are all independent of an investigation of the VPS. Those steps could all have been taken without access to the VPS. These steps should have been taken in any competent investigation of this type and no explanation is being offered by the Police evidence as to why these steps were not taken.

80. At paragraph 35, Mr Whale opines on the possibility of finding data from a search of Mr Hager's house notwithstanding the use of Tails software. I do not mean to be unkind to Mr Whale, but it appears from this paragraph that he is not actually familiar with Tails. He suggests that the user of the Tails software may have, by way of example, typed text into the wrong window – one "that was not protected by" Tails. He also says that the Windows operating systems copy information to temporary storage

locations all the time suggesting that this may create a forensic trail inadvertently. I strongly disagree with this evidence. Neither of these things are possible when one is using Tails.

81. Indeed, preventing these sorts of things is the design goal of Tails. One way in which this is achieved is that Tails operates as its own standalone operating system. This means that to use Tails, a person has to reboot their computer using just the Tails software. The computer will then be operating in the Tails operating system and Windows (or any other operating system) will not be running on the computer at all. If one is using Tails, there is therefore no possibility that any information will be inadvertently created by Windows since Windows will not be running on the computer at the time. Nor could one write in the wrong window. All windows will be running under the Tails operating system. No expert who knows what Tails is could make the claims that Mr Whale is making.

82. Tails also achieves its design goal in other ways. These make Mr Whale's evidence even more inaccurate. Tails does not use swap files and temporary storage locations. This is for exactly the reason that doing so might create the sort of forensic trail that Mr Whale is discussing in paragraph 35. Attached and marked as Exhibit "**AJB-3**" is a true copy of the introductory "About" page from the Tails website. Even that basic introductory page makes it clear that all of these statements from Mr Whale cannot be correct. The exact mechanisms that achieve this are described in more detail in the Tails documentation.

83. For the same reason, paragraphs 19, 20 and 32 of Mr Whale's evidence are based on either a misunderstanding of Tails or an unsupported assumption that the Leaker did not use Tails despite evidence to the contrary. When someone uses Tails, the software makes sure that any metadata that is created is anonymous. If one has a file that was created outside of the Tails system, then Tails provides a tool to enable the user to wipe any metadata that may have been created by that other system.

84. Again, without wishing to be rude, the problem is that Mr Whale does not have the correct expertise to be opining on these issues. Mr Whale is an expert in computer forensics. There was nothing in this case to forensically examine other than Mr Slater's computer, and all of the information in relation to that examination is being withheld from the Court. This comes back to the distinction I made in my first affidavit between computer crimes and crimes involving computers. Mr Whale's considerable expertise is in the latter. This case is about the former.

85. This case is about an alleged hack. If there was a hack then an investigator needs to consider the vectors by which it could have occurred and to look for the signs that such hacking techniques might have left. Looking at Mr Whale's list of expertise, as extensive and impressive as it is, there is nothing to suggest that these sorts of matters are within Mr Whale's skill set.

86. That is not to say that the inaccurate views that Mr Whale expresses about Tails require a particularly in depth knowledge of cybercrime. Anyone with basic computer knowledge would have been able to learn these things if they read the online documentation available for Tails. Indeed, as stated above, Mr Whale's fundamental misconceptions about Tails can be dispelled by just reading the introductory about page from the tails website. The importance of Mr Whale's lack of relevant experience is that everyone who works in this field would have already heard of, and been familiar with, Tails.

87. Even if one takes Mr Whale's evidence at its highest, I note that he does not go so far (in his paragraphs 33-36) as to say that the Police had reasonable grounds to believe that they would find evidence. The highest he puts it is that it was an avenue of investigation that "could" identify the Leaker. He appears to be putting it at the level of a possibility.

88. As per my first affidavit, I accept that it is possible that Mr Hager and the Leaker made some error and that there was such evidence at the house available to be found with this search. However, I stand by my view that,

while possible, the information available to the Police at the time of applying for the warrant suggested that the chance was very small.

Joseph Eng-Hoe Teo

89. Det Teo says in paragraphs 23-32 that the VPS that comprised the whaleoil website was not available from Linode and that Mr [redacted] had not taken a copy. At paragraphs 33-35, he suggests that this is a complete answer to all of my points raised in paragraphs 54-86 of my first affidavit. It is not.

90. First, Det Teo states that when the website was moved, Mr [redacted] took a copy of the website data but not the access data (23.6). I believe that this is an error. This was a website built using the WordPress software package. WordPress stores the website content (the articles etc) in a database. Most, but not all, of the access information is stored in a separate set of "log files". It appears from Det Teo's description of his conversation with Mr [redacted] that the content database must have been copied, but allegedly not the rest of the files which comprised the VPS, including the log files.

91. Indeed, a cursory glance at the website shows that website data was preserved. The blog articles archive is still there dating back to June 2005.

92. While the lack of the log files would mean that much of the access information is unavailable, it is not correct to say that no access information is available. The content database of a WordPress website also contains some access information. As one example, it includes account creation including the IP address at the time of account creation. So, for example, if the Leaker gained access by creating a new admin account (rather than using the login details of an already existing account) then this information would be in the content database. It is quite plausible that there would be a number of other useful pieces of information in this database.

93. Secondly, it is my view that Det Teo's efforts to obtain the VPS fell short of what might reasonably be expected. While he says that Mr [redacted] did not take a copy, he makes no effort to obtain a list of people who had access to it to discover if anyone else might have taken a copy. As discussed in my

first affidavit, Mr [redacted] says he lacked expertise and therefore had assistance from others to do this work. Yet, no attempt was made to find out who these people were or to talk to them.

94. Thirdly, Det Teo is wrongly conflating all of my discussion about the first scene of the crime with the VPS. The importance of the first scene of the crime evidence relates to all the various investigative techniques that would be undertaken with respect to the website. The VPS was only the first such investigation I suggested. The other potential avenues of investigation I identified did not depend on the availability of the VPS. For a start, the steps that I identified at paragraphs 83-86 of my first affidavit did not require access to the logs in the VPS. These inquiries involved asking Linode for business records held by Linode.

95. Det Teo's reply also fails to address any of the points I made in 87-94, which also relate to the first scene of the crime. Again, these lines of inquiry do not require access to the VPS. Therefore, even if Det Teo is correct to say that the VPS was inaccessible, all of these avenues of investigation remained open to the Police.

96. At paragraphs 23.9 and 23.10 of his affidavit, Det Teo states that he arranged for the Police to speak further with Mr [redacted] and that this happened after the search. No documents have been provided that provide information about these further conversations with Mr [redacted] Given Mr [redacted]s involvement, such further documents could have provided me with more details information about the website, which may have enabled me to provide better evidence on what investigative steps were still available to the Police. However, I note that the further conversation with Mr [redacted] was itself an investigative step. That step had been identified by the Police prior to the search, as per paragraph 23.9, but was not attempted until after the search as per paragraph 23.10. This appears to directly contradict the claims by DI Lynch and DS Beal that there were no such steps available to them at that time.

Rex Arthur Cottingham

Paragraph 7

97. For clarity, I point out that Mr Cottingham's reference to the "Onion Ring" exit nodes in paragraph 7 is clearly meant to be a reference to the Onion Router (TOR).

Paragraph 11

98. Mr Cottingham noted, in his paragraph 11, a number of further steps in relation to the lines of inquiry the Police were pursuing that he recommended they take. As noted above, in relation to Mr Whale's evidence (and by reference to Det Teo's evidence), some of these steps were never completed. In addition, I can see nothing in the documents to show that Mr Cottingham's suggestion at 11.7 was ever pursued.

99. I have been asked whether it was accurate to say that the uncompleted steps at the time the search warrant was applied for could not have been completed for "an extended period of time"/"some months". I do not know how long it takes to do a Mutual Assistance application or to obtain a US Court order. However, once such documents were obtained, it would have taken Twitter and Google very little time to comply with these orders. I also note that Mr Cottingham said in his jobsheet (**PD 11/2123**) that the Police could have asked for the FBI's assistance to obtain the Google data.

100. Also, the newly disclosed documents include an email exchange with Wikisend (**PD 14/2321-2328**). This is the line of inquiry suggested in Mr Cottingham's paragraph 11.8 and Mr Whale's paragraph 25(g). The timestamps on that exchange shows that that enquiry was still being carried out after the search warrant was obtained. The documents do not show when Wikisend provided the requested logs. However, the Police email requesting the logs is timed at 7:41 am on 2 October 2014, the day of the search (**PD 14/2326**). It therefore appears that the logs were received either during or shortly after the search and the Police analysis of those logs would have taken only a short time thereafter. It is possible that Wikisend

did not reply promptly to the email sent at 7:41 am, but I see no way that DI Lynch and DS Beal could have known that that would be the case on 30 September 2014.

101. In respect of the media inquiry suggested at Mr Cottingham's paragraph 11.7, I do not know how long the media would have taken to respond to the request, but the follow up search for the IP addresses related to the email accounts could have been done as quickly as all of the other IP address requests that the Police had been making through September 2014.

Paragraphs 15-17

102. At paragraphs 15 and 17, Mr Cottingham makes the point that an examination of access logs for the website may not have been fruitful. This is correct. However, the steps that the Police did pursue had an even lower prospect of being fruitful (including but not limited to the search of Mr Hager's house).

103. At paragraph 16, Mr Cottingham suggests that it would have been impractical to look through logs because of the number of legitimate accesses and because the Leaker could have been using legitimate login credentials. I strongly disagree with this evidence.

104. First, Mr Cottingham is exaggerating the number of login credentials that would need to be searched. Given the nature of the information that was obtained, if this was done through such a login, it would have needed to be a login using an account with administrative or privileged access. This significantly limits the list of user logins that would have needed to be checked.

105. Secondly, it is not in fact that difficult to quickly check through a large list of login information. The Police were searching for signs of logins from suspicious IP addresses, or otherwise unusual access. Even if there were a large list containing predominantly legitimate accesses, these legitimate accesses could have been very rapidly eliminated by reference to the fact,

for example, that they were made using a known IP address of a legitimate user.

106. Thirdly, the type of analysis that Mr Cottingham is suggesting was unfeasible in relation to the website login information is exactly the same as the ones that the Police decided to pursue in relation to the login information for Mr Slater's Google and Facebook accounts.

Time to undertake the steps I proposed in my first affidavit

107. Above, I expressed my view as far as I was able about whether DI Lynch and DS Beal were correct to say that, at the time of the search, other avenues of investigation were not going to bear fruit for some time. I did this purely in reference to the investigations that the Police were carrying out and therefore knew about at the time. I have also been asked to say whether this statement is true in relation to the avenues of investigation that I said in my first affidavit should have been pursued but which were not pursued.

108. This statement would certainly not be true in relation to those avenues of investigation. Those avenues of investigation could have been completed as quickly and easily as any of the ones that were pursued during the course of September 2014. They would not have taken months to complete.

Conclusion

109. As stated above, my conclusion is that my original opinions were correct. The Police had obvious avenues of investigation that they could have pursued but did not pursue. The Police were very unlikely to find evidence from a search of Mr Hager's house. As stated in my first affidavit, there are also good reasons to believe that the Police knew that it was very unlikely at the time of the search.

110. Many of the Police witnesses purport to dispute my first affidavit. However, there is in fact little actual contest between my evidence and theirs with respect to these overall conclusions.

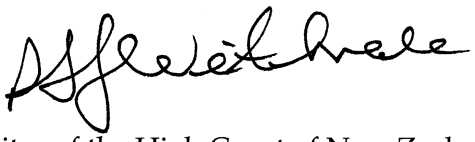
111. The Police dispute my evidence in relation to the VPS. I think they have made errors in respect of that line of inquiry. The Police dispute my view that they ought to have investigated insiders. I do not believe their reasoning is valid. However, putting those issues to one side, there is no dispute from the Police that all of the other avenues of investigation I identified were open to them.

112. In respect of the likelihood of the search being successful, the Police have given their reasoning for thinking that it might have been fruitful. Again, I dispute their reasoning. However, there is little challenge to my reasoning that suggests that the likelihood was very low. Nor does the Police evidence appear to respond directly to my reasoning that suggested that they knew this at the time of the search.

113. The Police do not appear to dispute that they knew the things about the Leaker's use of Tails that I have set out in my first affidavit. The only direct challenge to my reasoning appears to be from Mr Whale. This challenge is based on a fundamental misunderstanding on Mr Whale's part about what Tails is and how it works. Even then, Mr Whale's conclusions go no higher than to say that it was possible that the Police would find evidence. Mr Whale was also not involved in the investigation. None of the people involved in the search have therefore chosen to refute my evidence on the issue of their knowledge at the time of the search.

Affirmed in Wellington)
on the 16th day of June 2015)
before me)

Adam Julian Boileau



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

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***

Affidavit of [redacted]

Dated: 27 March 2015

Solicitor
Thomas Bennion
Bennion Law
L1, 181 Cuba Street
PO Box 25 433
Wellington 6146
Tel: +64 4 473 5755
Fax: +64 4 381 3276
tom@bennion.co.nz

Counsel
Julian Miles QC
Richmond Chambers
L5, General Buildings
33 Shortland Street
PO Box 1008
Auckland 1140
Tel: + 64 9 600 5504
miles@richmondchambers.co.nz

Felix Geiringer
Terrace Chambers
No. 1 The Terrace
PO Box 10 201
Wellington 6143
Tel: +64 4 909 7297
Fax: +64 4 909 7298
felix.geiringer@terracechambers.co.nz

190A

I, [redacted], student of Wellington, solemnly and sincerely affirm:

1. I live at 73 Grafton Road, Roseneath, Wellington. I live there with my father, Nicolas Alfred Hager, the applicant in these proceedings.

2. I make this affidavit to record some of the aspects of the execution of the search warrant and its impact on me.

3. On the morning of 2 October 2014, I was woken at 7.45 am by loud banging on the door. At that time, I was asleep in my bed.

4. I came to the front door. I was wearing only a light nightgown. I was half asleep. I expected it to be someone like a courier and that I could deal with them without fully opening the door.

5. When I opened the door I saw police officers there. One of the police officers told me that they had a search warrant. I looked at the search warrant and their identification.

6. I explained that my father was away. I was told that they were going to execute the warrant anyway. I told them I wanted to call a lawyer. They agreed to wait while I did that.

7. I tried to call Steven Price, who is a lawyer who does work for my father. However, Mr Price did not answer his phone.

8. The police then cautioned me. They told me that they were looking for electronic equipment. I asked what my rights were in relation to my computer. The police told me that the search warrant gave them the right to search any electronic equipment in the property. They made no mention of privilege.

9. I then called my father. I told him what was happening and then handed the phone over to Detective Sergeant Beal so that my father could speak with him.

10. After that call, I understand my father tried Mr Price again and managed to get in touch with him. My father rang back and told me that Mr Price would be coming over. Mr Price arrived a short while later.

11. During all of that, I was standing in the entranceway to my house with the police officers still only wearing my nightgown. I told the police officers that I wanted to get dressed. They told me that I had to get dressed in front of a police officer because they had not searched the house yet. I asked to be able to get dressed alone in the bathroom. I was told that I still had to get dressed in front of a police officer because they had not searched the bathroom.

12. I was not happy about having to do that. I thought it was totally unnecessary and needlessly intrusive. The idea that my father had a document showing Rawshark's identity hidden in our bathroom, in a location known to me, and that I was going to destroy it using the fact that I was undressed as a pretext, was utterly ridiculous.

13. I dressed in the bathroom in front of a female police office. I found this embarrassing.

14. In general, the officers were polite. However, they conducted an intense search of the house. The search was highly intrusive.

15. One of the first parts of the house the Police searched was my bedroom. The search included an officer going through my personal belongings, such as underwear. Again, I thought the idea that there was a realistic prospect of the Police finding what they were searching for in my underwear drawer was absurd. I found this very intrusive. I did not like having the police rifle through my underwear. It was an unnecessary invasion of my privacy.

16. The search of my room also included going through my private papers, including birthday cards and private letters, and my university books and papers. They looked through my private photo album. Again, I do not understand how they thought that there was a reasonable prospect of finding what they were looking for in any of that material.

17. I found the search of my room upsetting. I had watched the start of that search, but it became too upsetting and I had to leave. I therefore do not know the full extent of what they searched through in my room, but it appeared to be a thorough and highly invasive search.

18. From my bedroom the Police seized my laptop, two mobile phones, and an iPod. These were all my property. I told them that they were my property. It should have been obvious that they were my property given their location. I also assured them that there could not have been any relevant material on the phones and iPod. The phones had not been turned on for years. I told them that, but they insisted on seizing them all anyway. They also cloned my smartphone (which I had had one me during the initial parts of the search) and all the USB storage devices they found in my room and returned them later that day.

19. When I was discussing with the Police whether they were going to seize my laptop, they asked me to conduct some searches on it. They told me what to type and I typed what they said. At no point, did I give the Police permission to use my laptop in any way. Once it became clear that they were going to seize the laptop, Mr Price told them that privilege was claimed in relation to its contents. My understanding is that while Mr Price and I did not believe that the laptop contained anything of relevance to the Police, to the extent that we might be wrong, the material they were seeking was necessarily privileged.

20. There was no possible way that my smartphone contained any information relevant to this search. Privilege was not claimed on my smartphone. As a result, the Police examined all of the data on my smartphone.

21. More than any other part of this search, the search of my smartphone has caused me to feel violated. The Police printed out lists of all of my private contacts. The smartphone contained a year's worth of text messages, Facebook messages, emails, and messages from another social media service - WhatsApp. This included messages between me and my boyfriend of a

private nature. The idea that these messages were being reviewed by the Police has caused me substantial distress.

22. The search occurred two weeks before my final university papers were due. The papers were honours papers for my history degree. They were therefore both challenging papers and important papers for my future prospects. In particular, I was concerned about needing high enough grades to qualify for a master's scholarship. It was therefore a very stressful time even without the search.

23. The laptop seized by the Police contained the only drafts for all of my final essays. They talked about taking the laptop away and sealing it, or maybe cloning it at some unknown point in the future. In the event, it took over five months for the laptop to be returned. Without my files, this would have been a total disaster for my degree. Over the next two weeks, I had to hand in over 12000 words worth of work. I could not possibly have recreated that work in that time.

24. Felix Geiringer, another lawyer who had been doing work for my father, was called by Mr Price and came to the house to assist. Mr Geiringer asked the Police whether they could allow me to remove some files from the laptop. After some discussion, the Police agreed. The Police had found a blank disk in my bedroom. One of the police officers supervised me while I copied my drafts and one or two other documents, about six documents in total.

25. This made it possible for me to complete those courses. However, it was still a considerable inconvenience to lose my laptop at that point in my studies. I had to find someone to lend me one that I could use to complete the work. It took me a few days to arrange that. The laptop I borrowed was an old one and one I was not familiar with using. Its use therefore caused ongoing frustration for me over the following five months. It was a deeply annoying laptop.

190E

26. This was a substantial additional stress at a time when I was already experiencing considerable stress. It also wasted some of my time when I was rushing to complete my course work to meet deadlines.

27. While I copied the files I needed for the urgent work that had to be completed that fortnight, over the following five months, the absence of my other files caused me difficulties in relation to my course work.

28. As with the other searches, I do not accept that the seizure of my laptop was reasonable. The basis for seizing it was that I had a draft of *Dirty Politics* on my laptop. I cannot see how this gave the Police a reasonable prospect of finding Rawshark's identity.

29. As I said, it took over five months before my laptop was returned. I did not have access to many of my documents, photographs, and music during that time. As I think is true of many people nowadays, a large part of my life relies on and is connected to information stored on my personal computer. The seizure of my laptop was a significant intrusion on my private life.

30. The police search lasted for over ten hours. I found the experience exhausting and upsetting.

31. In the event, the practical and emotional disruptions meant that I was unable to complete two of the course requirements that were due that fortnight to what I believe to be a sufficient standard. However, I was able to explain the situation to the University and received an extra week for those requirements.

32. While I was present, the police officers promised Mr Price and me that they would be seizing and sealing material, and that they would not examine it unless and until they were permitted to do so by a judge after a judicial review. They made it clear that until such a time they would not be using it in the investigation.

33. I have been asked to say whether I gave the Police permission to deviate from that arrangement. I absolutely did not give them any such permission. I find the idea that they may have breached that promise to be upsetting.

34. At one point in the search, I answer questions from the police officers about an internet cable in the house. I did not fully understand what it was that were doing with it. I certainly did not do that to help them do anything that was inconsistent with the promise not to be examining any of the seized material. I do not recall them asking for permission to use the internet.

35. I understand that the Police may have breached this promise. If they did so, it was done out of sight and out of earshot of Mr Price and me. I am angry and upset that they would have done this. There was no room for misunderstanding this promise. It was made repeatedly and very clearly and it was discussed.

36. The Police also agreed to show Mr Price and me all photographs taken during the search. This was because we were concerned that the photographs themselves might contain privileged information, such as a photograph of a privileged document. The police officers had said that these were scene photographs and that they were not going to be used in the investigation in that way. However, the police officers agreed to let us review the photographs and said that if we identified any such photographs they would be deleted.

37. They showed me and Mr Price some photos. There was a clear understanding that we were being shown all of the photographs taken at the scene for the above purpose. I now understand that there may have been photographs taken that were not shown to me at that point. That is definitely inconsistent with the process that we had agreed. I understand further that those photographs include close up photographs of documents over which my father was claiming privilege. That is exactly the sort of document that we were concerned about and the whole point of the exercise was to identify such documents and have them deleted. What we were doing and why we

were doing it was very clear. There could not have been any misunderstanding.

38. During this process, Mr Price and I identified several photographs that we believed needed to be deleted. The police officers agreed to delete the photographs we identified with one exception. I took a second look at the disputed photograph and decided, on reflection, it wasn't a problem.

39. I do not remember viewing a photograph of a side of a phone and of a phone box. However, it is possible that I saw such photographs and did not think of their possible relevance. Nevertheless, as stated above, it was my understanding from what the police officers had told me and Mr Price that they would not be investigating anything based on the numbers on the side of such a box.

40. It is absolutely not possible that they showed me close up photographs of documents showing addresses and password details, and that I missed them or did not understand their relevance. I am 100% certain that the photographs that I reviewed did not contain any such photographs. Indeed, they did not contain any close up photographs of documents. If I had seen such a document I would definitely have told them to delete it.

41. I was also never shown any photographs of the screen of my laptop computer.

42. I understand that the Police accessed my laptop after they had told me that they were seizing it for cloning, and after they knew that privilege was claimed. They did not have any authority from me to do that.

Affirmed at Wellington)
on the 27th day of March 2015) [redacted]
before me)

PSJ Withnall

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

190H