

## 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**

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

jc  
fel

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.

A handwritten signature in blue ink, consisting of a stylized 'J' followed by a flourish.

### **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.

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.



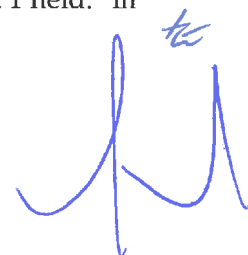
62. Among the specific incidents was the discovery that RNZAF had illegally transported a chemical pyrotechnic canister on an international Air New Zealand passenger flight to Canada, endangering the lives of all on board including up to 379 passengers. RNZAF had never reported the incident to Air New 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 than 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.

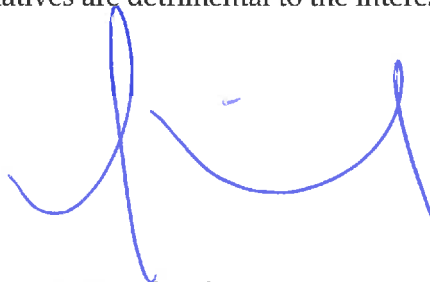
## Nicky Hager

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 27<sup>th</sup> day of March 2015)  
before me                           )



I Esekiele

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


# The New Zealand Herald DJF-1



**David Fisher**

David Fisher is a senior reporter for the NZ Herald.

5:30 AM Saturday Dec 1, 2012

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

## Police checks routine work for banks

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Police would not say how often banks gave them information.

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

information "subject to an obligation of confidence".

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

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

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

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

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

### **Cops' query hurt Dotcom loan**

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

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

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

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

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

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

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


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

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

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

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

- NZ Herald



2/2

# The New Zealand Herald



**David Fisher**

David Fisher is a senior reporter for the NZ Herald.

5:30 AM Saturday Dec 8, 2012

## Banks unite in silence on giving client details to police



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

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

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

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

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

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

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

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

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

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

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

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

He also questioned whether banks would be qualified to judge.

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

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

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

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

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

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

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

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

- NZ Herald

*[Handwritten signature]*  
1/1



# The New Zealand Herald



**David Fisher**

David Fisher is a senior reporter for the NZ Herald.

11:49 AM Wednesday Mar 25, 2015

## Police given personal information without search warrants

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



Assistant Police Commissioner Malcolm Burgess. Photo / Richard Robinson

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

to [signature] 1/2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- NZ Herald



2/2