IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY

CIV-2014-485-11344

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**
BETWEEN	**NICOLAS ALFRED HAGER**
	Applicant
AND	**ATTORNEY-GENERAL**
	First Respondent
AND	**THE NEW ZEALAND POLICE**
	Second Respondent
AND	**THE MANUKAU DISTRICT COURT**
	Third Respondent

FIRST AND SECOND RESPONDENTS' SUBMISSIONS

8 July 2015

Judicial Officer: Brown J
Next Event Date: 13 July 2015

CROWN LAW
TE TARI TURE O TE KARAUNA
PO Box 2858
WELLINGTON 6140
Tel: 04 472 1719
Fax: 04 473 3482

Contact Person:
Brendan Horsley / Kim Laurenson
Email: brendan.horsley@crownlaw.govt.nz / kim.laurenson@crownlaw.govt.nz

CONTENTS

1. In early 2014, blogger Cameron Slater's computer was unlawfully accessed by a hacker. Private and work related material was stolen. The applicant obtained the material from that hacking and used it to publish the book *Dirty Politics* in August 2014. *Dirty Politics* was widely discussed in New Zealand in the lead-up to the 2014 general election. More material from the hacking, including private information, was later published online by someone who called themselves Rawshark. Mr Slater complained to Police about the unlawful access to his information. Police investigated that complaint and as part of their investigation, executed a search warrant at the applicant's house on 2 October 2014.

2. The applicant has brought a wide-ranging challenge to the Police investigation of this offence, including the decision to apply for a warrant, obtaining a warrant, the execution of it and other steps taken in the investigation in relation to the applicant's information.

Summary of argument

3. This was a lawful search conducted by virtue of a properly issued search warrant. Search warrants to obtain material held by a journalist are permissible and a statutory process exists to allow for a Court to consider any claim to journalistic privilege that might be made. Such consideration can take place after the material has been seized but prior to any search of it. That was the entirely orthodox process followed here.

4. Police had reasonable grounds to believe that the search would find evidential material in respect of the offence. Those grounds were fairly disclosed in the application made to the District Court Judge. The applicant's ability to claim privilege in the material remained to him, and he chose to exercise it. The search itself was carried out in as minimally intrusive way as possible.

5. The material seized is now sealed in the High Court pending the resolution of this judicial review and a determination of the applicant's claim to privilege if this judicial review is unsuccessful. The full argument on the privilege claim is therefore yet to be heard and does not arise in these proceedings.

6. The first and second respondents' position is that:

6.1 In the absence of bad faith, the steps taken by Police to advance an investigation are not justiciable.

6.2 Search warrants are only judicially reviewable in certain limited circumstances which are not met here.

6.3 There is no requirement for a proportionality assessment by Police before applying for a warrant as the test for obtaining a warrant strikes the balance that is to apply.

6.4 Sufficient grounds for a warrant were before the Judge who issued the search warrant and the warrant was lawfully issued. There was nothing in the search warrant that was misleading and the Judge must have been alert to the potential for journalistic privilege to be an issue.

6.5 Journalistic privilege is recognised and protected by the New Zealand statutory regime, in particular s 68 of the Evidence Act 2006 and Part 4, subpart 5 of the Search and Surveillance Act 2012 ("SSA"). Those protections were appropriately utilised in this case. The application for the warrant and the steps that were taken during and after the warrant were largely compliant with the relevant legislation. The material that was seized was not searched but was instead sealed and was delivered to the High Court.

6.6 The statutory framework contemplates that a Court will make a determination of the public interest in the disclosure of the information over which privilege is claimed as opposed to the adverse effects and the value of disclosure. An application to have that question determined has been made and is on hold pending the outcome of this judicial review. In the absence of a certainty that Police could not make out the s 68 test for disclosure, it is not wrong for Police to seize but not search material potentially privileged material.

6.7 The search was conducted in a reasonable way and the disruption to the applicant minimised as much as possible. Proposals to allow for

the copying and return of the applicant's property have been made but not accepted by him.

6.8 Other steps taken in the investigation in relation to the applicant were lawful.

Relevant factual matters

Complaint of unlawful access to Mr Slater's computer

7. Mr Slater runs the blog Whaleoil Beef Hooked ("Whaleoil"). Whaleoil was found to be a news medium for the purposes of s 68 of the Evidence Act and a determination was made by the Court in that case that Mr Slater had himself received information from informants as a journalist in the normal course of work.[1] On 19 August 2014 he complained to Police that his computer had been hacked in February 2014. Mr Slater's email, Facebook and Twitter accounts had been accessed and information found in them were now the subject of the *Dirty Politics* book published by the applicant. He said that unlawfully accessed material included material that was private and privileged, including material sent between him and his lawyers and medical professionals.[2] It also included material sent to him and by him as a result of his work on the Whaleoil blog, including from journalists and Members of Parliament. Mr Slater did not give the applicant or other members of the media permission to publish any of this material.

8. The applicant is a well-known journalist. His book *Dirty Politics* was published on 13 August 2014 and was based on the material obtained from Mr Slater[3] without Mr Slater's permission or knowledge. In the preface to the book, the applicant said that he received the source material that formed the basis of the book "out of the blue" on a USB stick.[4] It seems the applicant no longer maintains that the receipt of the material was out of the blue but in fact says he became aware it was available and asked to be given a copy.[5] The material in

---

1 *Slater v Blomfield* [2014] NZHC 2221

2 Cameron Slater complaint to Police appended to the affidavit of Linda Cheesman at v 8, at p 1441, search warrant application LMC volume 8 at p 1528, and Cameron Slater email to Police, appended to the affidavit of Linda Cheesman vol 14 at p 2248

3 Affidavit of Nicolas Hager para 66.

4 *Dirty Politics* at p 12.

5 Affidavit of Nicolas Hager paras 59 to 65.

the book included direct quotations from emails and other communications between Mr Slater and people who provided him with material for his blog.[6] *Dirty Politics* received a lot of public attention in the lead up to the 2014 general election.

9. After *Dirty Politics* was published, the source material from it began appearing online on a Twitter account called "Whaledump". This material included material that the applicant had left out of his book on the basis that Mr Slater's 'right to privacy outweighs any public interest'.[7]

Police commence an investigation

10. Following Mr Slater's complaint, Police commenced an investigation into an offence against s 249 of the Crimes Act 1961, accessing a computer system for a dishonest purpose, and in particular into the identity of the hacker. That offence carries a maximum penalty of seven years of imprisonment. The investigation team assigned to investigate the complaint were based in Counties Manukau due to the fact that Mr Slater's computer was in that district when the hacking took place.[8]

11. The investigation was assigned to Detective Sergeant Simon Beal, with oversight from Detective Inspector David Lynch, the Counties Manukau District Manager, Criminal Investigations.[9]

12. Detective Sergeant Beal put together an investigation plan outlining the steps to be taken in the investigation and Police began to investigate the offence by taking a number of steps including interviewing Mr Slater, reviewing open source material, making requests of companies and agencies that might hold relevant information and conducting technical inquiries, some with the assistance of the Police National Cyber Crime Centre.

13. When interviewed by Police on 29 August 2014, Mr Slater said he did not know who the hacker was. He explained to Police that his blog had been the subject of a "denial of service" attack in February 2014 but he was not able to

---

6 *Dirty Politics* at p 13.

7 *Dirty Politics* at p 13.

8 Affidavit of David Lynch at paras 6 to 8.

tell at that time how much of his information might have been accessed.[10] He said that he did not know who had hacked his computer and he had not given Mr Hager permission to publish his material. Police obtained Mr Slater's computer from him on 15 September 2014 and it was examined by the Police Electronic Crime Lab ("ECL").[11] Before the search warrant was executed, Detective Sergeant Beal had been informed that it was unlikely that any information of use to the investigation would be able to be found from the examination of Mr Slater's computer.[12] This was later confirmed.[13]

14. Police involved technical experts from the National Cyber Crime Centre ("NC3"). Staff from NC3, in particular Mr Rex Cottingham, suggested to the inquiry team in Counties Manukau various technical inquiries that might be useful.[14] Mr Cottingham assisted with actually carrying out some of those inquiries.

15. Police were aware of IP addresses that were obtained from Mr Slater when his accounts were being targeted. Police made requests, by way of production orders and information requests, to Orcon Internet Limited, Yahoo, Twitter, Facebook and Wikisend to attempt to follow lines of inquiry relating to Mr Slater's email, Facebook and Twitter accounts, the known IP addresses, and the Twitter account that had been used to publish the hacked material online.[15] Some these inquiries generated leads, but ultimately did not identify a person of interest. Other inquiries were not fruitful because they did not generate any information at all.

16. Police also spoke to [redacted] Mr Slater's technical support person, on 30 September 2014. Following that conversation, further inquiries were made with the company that hosted the Whaleoil website, Linode. It was not

---

9 Affidavit of David Lynch at para 9.

10 Cameron Slater complaint to Police appended to the affidavit of Linda Cheesman commencing at v 8 p 1441, at p 1448.

11 Affidavit of Simon Beal at para 12.

12 Supplementary affidavit of Simon Beal at para 1.

13 Affidavit of Simon Beal at para 12.

14 Affidavit of Rex Cottingham at para 10.

15 Affidavit of Rex Cottingham at paras 10 to 11, affidavit of Joseph Teo at paras 8 to 15.

possible to obtain the Whaleoil website logs which might have assisted the investigation from Linode due to the passage of time.[16]

17. Given the remarks made by the hacker publically that if he was caught he would face seven years in jail, Police focussed on people who did not have legitimate access to the material. A person with legitimate access would be unlikely to accept that they had committed an offence of that kind.[17]

18. Expert evidence filed by Police from Mr Brent Whale suggests that Police carried out appropriate and wide-ranging inquiries into the hacking.[18] Mr Whale also observes that merely because a person takes security precautions, it does not mean that no evidence will be found if their electronic system is examined.[19] To similar effect is the evidence of Detective Inspector Lynch that even a careful person can leave an electronic trail that Police can later detect.[20]

19. Police reviewed publically available material, including the Whaledump Twitter account and interviews the applicant gave other members of the media. Police on the investigation team were aware of Sean Plunket interviewing the applicant on Radio Live on 14 August 2014 and in particular the applicant's acceptance in that interview that the hacker was someone he knew and that he did not want to disclose their identity because 'they would get in trouble with the Police and I've promised to keep their identity a secret'.[21] Police also noted the applicant's interview with Susan Wood on One News on 17 August where he said "I was advised by my lawyer that I should return all my materials to my source because a court judgment could come out which might mean I might be forced, because it is a book to hand over all the material and expose my source".[22] Police could not identify any comments from the applicant that suggest he did in fact take the advice and return the material.

---

16 Affidavit of Joseph Teo at paras 23 to 32.

17 Affidavit of David Lynch at para 74.

18 Affidavit of Brent Whale at para 36.

19 Affidavit of Brent Whale at para 35.

20 Affidavit of David Lynch at para 38.

21 Affidavit of Simon Beal at para 7.

22 Affidavit of Simon Beal at para 8.

20. Retired officer Police officer Wayne Stringer has been critical of the steps Police took in this case. It is submitted that those criticisms are answered in the second affidavit of Detective Inspector Lynch.

Decision to apply for a search warrant

21. Nearly six weeks after first receiving a complaint from Mr Slater, Police decided to apply for a search warrant for the applicant's house. That decision was made by Detective Inspector Lynch at the point where some lines of inquiry had reached an end and others were considered to be some months away from providing any information.[23] The next step was considered to be applying for a search warrant either over the applicant's house or the premises of other journalists who appeared to have had contact with the hacker.[24] The latter was rejected on the basis that the applicant was the only journalist who had openly admitted that he knew who the hacker was and was also in contact with him.[25] It was not clear that other journalists knew the identity of the hacker and keeping in mind the need to be cautious in executing a warrant over a journalist's premises, Police were reluctant to obtain those warrants as matters stood.[26]

22. Detective Sergeant Beal was tasked with applying for a warrant over the applicant's premises. Police obtained legal advice both on the application itself and the process for a s 68 claim and read applicable Police policy. It was considered impractical to announce the execution of the warrant to the applicant given his involvement in the subject matter of the offence.[27] Police considered that even if a person thought that they had removed electronic evidence, it could be possible for forensic examination to find that evidence.[28]

23. Police were alert to the fact that the applicant might claim journalistic privilege in respect of items at his house and were prepared to seal the seized material if that proved necessary.

---

23 Affidavit of David Lynch at para 32.

24 Affidavit of David Lynch at para 32.

25 Affidavit of David Lynch at para 34.

26 Affidavit of David Lynch at para 35.

27 Affidavit of David Lynch at para 54.

28 Affidavit of Simon Beal at para 32.

The execution of the warrant

24. The warrant was executed on 2 October. Six Police staff arrived at the applicant's address in Wellington at 7.40am. He was not home but his daughter Ms [redacted] was. Care was taken to ensure that the warrant was carried out in a reasonable way and the disruption minimised.[29]

25. Detective Sergeant Beal spoke to the applicant on the telephone as he was out of Wellington. The applicant had some concerns about the warrant being executed. Detective Sergeant Beal asked the applicant if he was claiming privilege over his property and he said he was. As a result, items to be seized were sealed by Police so that they could not be further examined until the claim to privilege was resolved. At least one of the applicant's lawyers were present during the execution of the warrant from 9.10am until Police left at 6.40pm.[30]

26. The items seized were sealed and delivered to the High Court for determination of the privilege claim.

Investigation after the warrant

27. The investigation into this offending is ongoing and Police continue to pursue various lines of inquiry. As it is set out further in these submissions at paragraphs 104 to 112, save for one exception, these lines of inquiry have not been taken in reliance on the privileged material.

28. No one has yet been charged in relation to the offending.

Legal proceedings

29. On 17 October 2014, an originating application was filed on behalf of Police in the High Court at Auckland seeking determination of the applicant's privilege claim and directions for dealing with the seized material. The High Court at Auckland was where the seized materials were, and are, held.

---

29 Affidavit of Simon Beal at paras 39 to 48.

30 Affidavit of Simon Beal at paras 46-48.

30. On 30 October 2014, the applicant brought these judicial review proceedings raising a wider range of issues and in particular alleging that the search itself was unlawful.

31. The first and second respondents considered that it would be logical to hear the judicial review proceedings first because, if the search was unlawful, then no question of privilege arises for determination and the originating application will not need to be determined. If, however, the judicial review is determined in the respondents' favour, then the originating application remains to be determined.

32. If the originating application leads to a determination that the s 68 test comes out in favour of disclosure of the material, then the Judge in that proceeding will be able to give directions on how the seized material is to be searched and who is to do that and so on.

Substantive submissions

Justiciability of search warrants and other investigative steps

33. This judicial review arises out of steps taken by Police in the course of an ongoing investigation into criminal offending. Whether or not Police should investigate a particular complaint, and if so, how to do so, have been issues where Courts have been reluctant to intervene. The argument for the applicant requires the Court to assess the sufficiency of the Police investigation. The applicant suggests both that a surprising number of resources were committed to the investigation[31], but also that Police should have committed resources to some investigative steps that were not taken. He is critical both of steps that were taken and those that were not. It is submitted that Courts have previously been reluctant to conduct this kind of close scrutiny of otherwise lawful actions by Police.

34. In *Evers v Attorney-General*, a claim that Police failed to investigate a complaint in a satisfactory manner was struck out.[32] The Court in *Evers* referred to *Hill v*

---

31 The applicant has suggested that 35 people were involved in the investigation. This is an overstatement of the facts. Only about six staff spent any significant amount of time on the investigation.

32 [2000] NZAR 372.

Chief Constable of West Yorkshire[33] and *R v Commissioner of Police of the Metropolis, ex parte Blackburn*.[34] In *Hill* the Court held:

> By common law police officers owe to the general public a duty to enforce the criminal law: see *R v Metropolitan Police Comr, ex p Blackburn* [1968] 1 All ER 763, [1968] 2 QB 118. That duty may be enforced by mandamus, at the instance of one having title to sue. But as that case shows, a chief officer of police has a wide discretion as to the manner in which the duty is discharged. It is for him to decide how available resources should be deployed, whether particular lines of inquiry should or should not be followed and even whether or not certain crimes should be prosecuted. It is only if his decision on such matters is such as no reasonable chief officer of police would arrive at that someone with an interest to do so may be in a position to have recourse to judicial review. So the common law, while laying on chief officers of police an obligation to enforce the law, makes no specific requirements as to the manner in which the obligation is to be discharged

35. To similar effect were the comments of the English Court of Appeal in *Blackburn*:

> Although the chief officers of police are answerable to the law, there are many fields in which they have a discretion with which the law will not interfere. For instance, it is for the Commissioner of Police of the Metropolis, or the chief constable, as the case may be, to decide in any particular case whether inquiries should be pursued, or whether an arrest should be made, or a prosecution brought. It must be for him to decide on the disposition of his force and the concentration of his resources on any particular crime or area. No court can or should give him direction on such a matter. [35]

36. The kind of thorough examination of the steps taken by Police that the applicant seeks here is not in accordance with the measure of discretion that Police have in investigating crime.

37. Search warrants are in a different category from the Police exercise of broader investigative powers and are of course regularly scrutinised by the Courts. However, judicial review of search warrants is only available in limited circumstances that are not easily made out here. Where, as here, experts disagree about the steps that Police could have taken and the likelihood of those steps being of assistance to the investigation and it is clear that the Police view is not entirely misconceived or not genuinely held, it is submitted that the

---

33 [1988] 2 All ER 238 (HL).

34 [1968] 2 QB 118 (CA).

35 *Blackburn* at p 136.

principles in *Blackburn* suggest the Court should be reluctant to substitute its own assessment.

38. In the leading case on the appropriateness of judicial review for challenging search warrants, *Gill v Attorney-General*, the Court of Appeal noted that judicial review of a search warrant may be available when the alleged defect in the warrant is of a fundamental nature, or where the jurisdiction of the issuing officer is challenged or some other ground of true unlawfulness such as want of jurisdiction is claimed.[36] The Court also observed the limited ability of the Court to conduct fact-finding in judicial review.[37] *Gill* was a case involving the search of a doctor's office, where doctor-patient privilege was at issue. The Court of Appeal dealt with an argument that judicial review was appropriate to maintain the confidentiality of patient records as follows:

> Mr Hooker for the appellants submitted that a challenge by way of judicial review was necessary so that Dr Gill could ensure that the confidentiality of patient consultation and other records could be maintained. He further contended that it was necessary to test the nature and scope of any privilege surrounding confidential information and records emanating from the doctor-patient relationship. Had this been the real purpose of the judicial review proceedings, we consider it could have been achieved by means of a succinct, focused statement of claim directed to those key points. An alternative approach would have been to negotiate with Ministry officials or its legal advisers suitable confidentiality undertakings pending the outcome of the investigation. But rather, a broadly based statement of claim sought to challenge many aspects of the application for the search warrant, its issue and execution.[38]

39. In *Southern Storm Fishing v Chief Executive, Ministries of Fisheries*, the Court of Appeal rejected the argument that the way in which privileged material was treated during a search amounted to a fundamental defect of the kind that could make judicial review appropriate on *Gill* principles.[39] The Court was prepared to assume, without deciding, that the treatment of privileged material during a search could go to the reasonableness of that search but nonetheless held that judicial review was inappropriate. The Court noted that it was 'relevant in assessing the court's proper response in an application for judicial review seeking a discretionary remedy that the officers did take steps to try to

---

36 [2010] NZCA 468 at [20].

37 *Gill* at [17].

38 *Gill* at [18].

39 [2015] NZAR 816 at [48].

protect privilege and any invasion was minimal' and that it was important that other remedies existed for the applicant. [40]

40. As set out further below in relation to the search warrant, there was no fundamental defect in this warrant of the kind that would make judicial review appropriate or necessary.[41] This statement of claim is not the 'succinct, focused' document for resolving privilege issues contemplated by the Court in *Gill*. The originating application that was already in train could have dealt with the narrow issue of whether a claim to privilege under s 68 can be sustained by the applicant.

Protection for journalistic privilege in New Zealand

41. Journalistic privilege is recognised and protected under New Zealand law. Parliament has framed the balance to be struck between journalistic privilege and other values that might from time to time conflict with it in s 68 of the Evidence Act as follows:

> 68 Protection of journalists' sources
>
> (1) If a journalist has promised an informant not to disclose the informant's identity, neither the journalist nor his or her employer is compellable in a civil or criminal proceeding to answer any question or produce any document that would disclose the identity of the informant or enable that identity to be discovered.
>
> (2) A Judge of the High Court may order that subsection (1) is not to apply if satisfied by a party to a civil or criminal proceeding that, having regard to the issues to be determined in that proceeding, the public interest in the disclosure of evidence of the identity of the informant outweighs—
>
> (a) any likely adverse effect of the disclosure on the informant or any other person; and
>
> (b) the public interest in the communication of facts and opinion to the public by the news media and, accordingly also, in the ability of the news media to access sources of facts.
>
> (3) The Judge may make the order subject to any terms and conditions that the Judge thinks appropriate.
>
> (4) This section does not affect the power or authority of the House of Representatives.

---

40 *Southern Storm* at [48].

41 In comparison to *A Firm of Solicitors v District Court at Auckland* [2006] 1 NZLR 586 and *Tranz Rail v Wellington District Court* [2002] 3 NZLR 780.

> (5) In this section,—
>
> informant means a person who gives information to a journalist in the normal course of the journalist's work in the expectation that the information may be published in a news medium
>
> journalist means a person who in the normal course of that person's work may be given information by an informant in the expectation that the information may be published in a news medium
>
> news medium means a medium for the dissemination to the public or a section of the public of news and observations on news
>
> public interest in the disclosure of evidence includes, in a criminal proceeding, the defendant's right to present an effective defence.

42. Section 68 recognises at subsection (2)(b) the right under s 14 of the New Zealand Bill of Rights Act 1990 to freedom of expression that journalists have in relation to receiving and imparting information. It also contemplates that that right might be overridden in certain circumstances.

43. The SSA provides the statutory framework for dealing with claims of privilege in the context of searches, including journalistic privilege, at ss 142 to 147.

44. It is plain that Parliament has contemplated that seizure of material where privilege is claimed can take place, subject to the power of the Court to then determine any claim of privilege: s 146.

45. It is submitted that New Zealand's particular statutory provisions make reliance on decisions from other jurisdictions difficult.[42] The enactment of the SSA also makes some of the authority that predates it of limited assistance.

46. The applicant makes an argument for Police conduct in relation to the search warrant to be assessed by virtue of a proportionality test under the Bill of Rights Act. The applicant's suggested approach is both novel and unsupported by case law. The statutory power to issue a search warrant is already crafted in such a way as to strike the balance between ss 14, 21 and the public interest in the detection and prosecution of crime. The majority of the Supreme Court reached a similar view of the test for a warrant in the Mutual Assistance in Criminal Matters Act 1992 in *Dotcom v Attorney-General*, noting that that the s 21

---

42 See for instance *Police v Campbell* [2010] 1 NZLR 483 at [89].

values were already built into the legislation.[43] The issue of the relevance of proportionality is discussed further at paragraph 67 below.

Assessment of s 68 in this case

47. If this Court finds the search here to be lawful and reasonable, then the next step will be to determine the applicant's claim to privilege in accordance with s 68. For the purposes of this judicial review, the first and second respondents say that s 68 is of some relevance to the legality of the warrant itself, but the ultimate determination of the s 68 claim is not required as part of this judicial review.

48. It is accepted that if it were plain that the s 68 analysis could not come out in favour of disclosure then it would not be proper for Police to obtain a warrant. To do so would be pointless, and could achieve nothing but temporary seizure of items which could not be searched and would then have to be returned to the journalist. However, this is not such a case.

49. The applicant could bring this matter under s 68(1) as he is a journalist. It was not necessarily plain at the time of the search that he had in fact promised confidentiality as required by s 68 (although he spoke to the media about discussions he had had with his source, *Dirty Politics* itself referred to the information having arrived 'out of the blue' and presumably therefore before any promise of confidence could be made).

50. Assuming a promise of confidentiality can be established, the balancing test under s 68(2) requires an assessment of the competing interests, namely the public interest in disclosure as opposed to the adverse effects. This exercise was considered in detail by Randerson J in *Police v Campbell.* The Court in that case was required to assess the competing arguments for the disclosure of the confession one of the suspects in an investigation into the theft of some war medals from a museum had made to journalist John Campbell. The Court began by noting the strong public interest in the investigation and prosecution of crime.[44] The argument that the s 68 exercise is a discretion and not a

---

43 [2014] NZSC 199 at [101].

44 *Campbell* at [72].

balancing test was rejected and the test in s 10 of the Contempt of Court Act 1981 (UK) distinguished by virtue of its significantly different wording.[45]

51. The Court in *Campbell* accepted, however, that there is a presumptive right for a journalist to protect a source that 'should not be departed from lightly and only after a careful weighing of each of the statutory considerations'.[46] It is relevant to consider whether other means are available to obtain the information sought, the significance of it to the prosecution case and the seriousness of the offending.[47] *Campbell* does not say that all reasonable alternatives need to be exhausted before the disclosure of a journalist's source can be considered, nor does it in fact deal at all with when a warrant can be applied for, it is directed to when the s 68 exercise will come out in favour of disclosure.

52. The applicant accepts that the offending alleged here was moderately serious. Police had already conducted a significant investigation and had been unable to identify the hacker. Identity was, of course, crucial to any prosecution. The applicant says that other steps could have been taken to identify the hacker but Police formed a different view. That dispute is at best a matter to be factored into the s 68 exercise and could not be conclusive.

53. There was public interest in this material as it appeared in *Dirty Politics*, relating as it did to the activities of various public officials. As the applicant says, the book received significant public attention in the lead up to the 2014 general election. There was little to no public interest in some of the material about Mr Slater's private life[48] that appeared online via the Whaledump account.

54. The Court is then to consider the countervailing considerations, namely any harm to the informant and the public interest in news and whether future

---

45 *Campbell* at [89].

46 *Campbell* at [96].

47 *Campbell* at [96] to [98].

48 See the description in the affidavit of David Fisher at para 56.

disclosures are likely to be impeded.[49] The Court then has a discretion to order disclosure or not.[50]

55. When considering the particular facts of *Campbell*, the Court observed:

> The usual case in which the protection of a journalist's sources arises is where an informant discloses evidence of wrong-doing by others, not by themselves. A person who confesses to a serious crime knowing that the confession will be broadcast to the public takes a very serious risk even if promised confidentiality. Such a person could not reasonably have a high level of confidence that the Court would protect his identity. Nor could a journalist reasonably believe the identity of the source would inevitably be protected.[51]

56. It is not clear from the applicant's evidence whether his source was the hacker or if his source had obtained the material from the hacker.[52] The applicant's statement on Radio Live that he was concerned his source would be in trouble with the Police[53] suggests the former. If the informant was the hacker, then it is submitted that this is a situation much like *Campbell* in that the informant has essentially confessed to a crime. Both the applicant and the informant must have known that there was a risk that disclosure would be required. There would be no illegitimate harm to the informant in that situation.

57. The High Court also had to consider the s 68 balancing test in *Slater v Blomfield* when deciding if disclosure of Mr Slater's informants was required as part of defamation proceedings. Asher J in that case observed:

> The way in which the sources have acted is also relevant in assessing the weight to be placed on the need to protect them. It was said in *X Ltd v Morgan-Grampian (Publishers) Ltd* in the context of a case decided under s 10 of the Contempt of Court Act 1981 (UK) by Lord Bridge:
>
> > But another and perhaps more significant factor which will very much affect the importance of protecting the source will be the manner in which the information was itself obtained by the source. If it appears to the court that the information was obtained legitimately this will enhance the importance of protecting the source. Conversely, if it appears that the information was obtained illegally, this will diminish the importance of protecting the source unless, of course, this factor is counterbalanced by a clear public interest in

---

49 *Campbell* at [100] and [101].

50 *Campbell* at [102].

51 *Cambell* at [112].

52 Affidavit of Nicolas Hager at para 59.

53 Affidavit of Simon Beal at para 8.

> publication of the information, as in the classic case where the source has acted for the purpose of exposing inquiry.[54]

58. The applicant says that he satisfied himself that the leak was not politically motivated,[55] but it is apparent that whatever the motivation, the material was obtained illegally and the importance of protecting the source of the information is accordingly diminished. The hacking may well have been motivated by malice but an objective assessment of the hacker's motivation is not possible until his or her identity is known. It appears to have been an external fishing expedition with a view to embarrassing Mr Slater. The release of the material via Whaledump reinforces that view. It was certainly not a whistle blower situation.

59. The first and second respondents argue that the s 68 analysis comes out in favour of disclosure. However, it is submitted it is not necessary to go that far in considering the legality of the warrant. The process to be followed is for material to be seized pending the s 68 determination. It is for a Judge, not Police, to assess the relevant s 68 factors. If the s 68 process is at least arguably going to be in favour of disclosure then it cannot be improper to carry out a search to seek to have that question ruled on by the Court.

Assessment of the effect on journalists' sources

60. It seems to be said for the applicant that the fact of this warrant being issued, even without the seized material being searched to date, will decrease the willingness of other confidential sources to come forward. It is said by some of the journalists whose evidence has been put forward by the applicant that in their opinion, the mere fact of this search having occurred will deter future disclosures. This, of course, is only a prediction, no witness going so far as to say that in fact journalists as a whole have had fewer confidential sources since October last year.[56] Such a decrease might not be expected given that to date no confidential source of the applicant's has been disclosed. Searches over journalists' material have always been possible, the search of the applicant's property has not altered that in any way.

---

54 *Slater v Blomfield* [2014] 3 NZLR 835 at [131].

55 Affidavit of Nicolas Hager at para 91.

56 Mr Fisher goes so far as to say he has observed a 'change in attitude' at para 43 of his affidavit.

61. Plainly, s 68 contemplates that in some circumstances, the public interest might outweigh a claim to journalistic privilege. The privilege is not absolute. That might deter some people from speaking to journalists, but that is the decision that Parliament has made. Whether or not such a disclosure should be made in this case falls to be determined by the Court when the s 68 issue is squarely before the Court pursuant to the originating application.

62. It appears likely that the hacker in this case committed an offence with a maximum penalty of seven years, at least a moderately serious offence. Parliament intends that people be deterred from committing crime. To the extent that the Police investigation in this case might deter others from committing hacking offences, it is submitted that is not a strange result. There is a distinction to be made here between people who lawfully obtain material and those who breach the criminal law in order to do so.

63. It is also noted that like the applicant, Mr Slater published news. People came to him with information about current events that was then published on his blog. Some of those people, and Mr Slater, have had material they considered to be private, widely published as a result of *Dirty Politics*. That may well have deterred them from speaking to Mr Slater or other media in the future. Whatever view might be held of Mr Slater's style of blogging, his computer system is protected from unlawful access by virtue of s 249 of the Crimes Act in the same way as that of any other person.

The decision to apply for a search warrant for the applicant's house

64. The applicant challenges not only the issuing of the search warrant but the decisions by Police to decide to seek a warrant and to apply for it.[57] The decision to seek a warrant and to apply for one would seem to be very much the same decision.

65. The first and second respondents consider that, in the absence of bad faith, the question of whether or not it was lawful to apply for a search warrant turns on whether or not it was lawful for one to issue. If it were lawful for the warrant to issue, then it is difficult to see how it could be improper to apply for one. If

---

57 Applicant's submissions at para 1.4.1.

it were not lawful to obtain a warrant, then whether or not it was lawful to apply for one is likely to be beside the point because the search will at that point be unlawful in any event.

66. Accordingly, while it is accepted that broad statutory powers are in principle read down to authorise only rights-consistent behaviour, on the facts as they arise here, the power to apply is so closely linked to the power for a warrant to be granted that the two largely fall to be considered together. If the warrant was lawfully issued then no proportionality assessment is required. Similarly, if the warrant was validly issued, in the absence of some event between the issue and execution that makes execution inappropriate, the decision to execute a warrant would also seem to be subsumed within the question of whether the warrant should be have been issued at all.

67. The argument for the legality of the application is therefore addressed below in the context of the legality of the warrant itself.

Search warrant lawfully issued

Application properly recognised a potential claim for privilege

68. Police applied for a search warrant under s 6 of the SSA. It was granted by the Judge. The applicant argues that it should not have issued because both Police and the Judge failed to give proper consideration to his rights and because the application did not make out the statutory test for a warrant.

69. In order to obtain a search warrant, Police must satisfy the test set out in s 6 of the SSA:

> An issuing officer may issue a search warrant, in relation to a place, vehicle, or other thing, on application by a constable if the issuing officer is satisfied that there are reasonable grounds—
>
> (a) to suspect that an offence specified in the application and punishable by imprisonment has been committed, or is being committed, or will be committed; and
>
> (b) to believe that the search will find evidential material in respect of the offence in or on the place, vehicle, or other thing specified in the application.

70. An application for a warrant is akin to an ex parte application and Police are obliged to put before the issuing officer, in a candid way, any facts that might count against the issuing of the warrant.[58]

71. The SSA sets out the way in which a privilege claim is to be dealt with. The privilege journalists can claim under s 68 is expressly included in the SSA regime (s 136(1)(i)). It allows for a person who claims privilege to prevent the search of a communication over which privilege is claimed pending the resolution of that claim (s 142). It sets down particular rules for search warrants over lawyers' premises, requiring that the lawyer be present or the Law Society contacted (s 143) and there are similar protections for the premises of ministers of religion, medical practitioners, and clinical psychologists (s 144). Being covered by none of the express conditions in ss 142 and 143, journalistic privilege is covered by s 145 which provides:

> 145 Searches otherwise affecting privileged materials
>
> (1) This section applies if—
>
> (a) a person executes a search warrant or exercises another search power; and
>
> (b) he or she has reasonable grounds to believe that any thing discovered in the search may be the subject of a privilege recognised by this subpart.
>
> (2) If this section applies, the person responsible for executing the search warrant or other person exercising the search power—
>
> (a) must provide any person who he or she believes may be able to claim a privilege recognised by this subpart a reasonable opportunity to claim it; and
>
> (b) may, if the person executing the search warrant or exercising the other search power is unable to identify or contact a person who may be able to claim a privilege, or that person's lawyer, within a reasonable period,—
>
> (i) apply to a Judge of the appropriate court for a determination as to the status of the thing; and
>
> (ii) do any thing necessary to enable that court to make that determination.

72. The SSA makes it clear that pending the resolution of a privilege claim, the thing in question can be secured (including by making a copy) and delivered to the Court but it cannot be searched (s 146). Section 147 then requires the

---

58 *Director of the Serious Fraud Office v A Firm of Solicitors* [2006] 1 NZLR 586 at [35].

person who claims the privilege to particularise the claim to privilege or apply to the Court for directions.

73. The SSA, then, provides a comprehensive regime for enforcement officers who search items over which privilege is claimed and requires them to give people an opportunity to claim privilege, not to search material when privilege is claimed and to deliver that material to the Court for safe keeping. Some of the conditions that the applicant suggests at paras 3.171 to 3.175 of his submissions as things that should have been required as part of the warrant were in fact implied as a matter of law, or are not consistent with the requirements of the SSA. For instance, there is a requirement in s 143 that when searching a lawyer's premises, that lawyer or his or her representative must be present. Similarly in s 144, when searching professional material held by a minister of religion, medical practitioner, or clinical psychologist, that person or their representative it to be present. The search of a journalist's premises is expressly contemplated by the SSA but similar protections are not extended to journalists.

74. It is submitted that the absence of those requirements for the search of a journalist's material must represent a deliberate choice on the part of Parliament and suggests that a similar condition will not always be required when a journalist's premises are searched.

75. Before the SSA, cases on searches of material covered by legal professional privilege indicated that conditions on a warrant ought to be imposed.[59] The case law prior to the SSA remains of application to the extent that it has not been overtaken by the provisions of the SSA. The leading case prior to the SSA on the principles to be considered when assessing search warrants over media organisations is *TVNZ v Attorney-General*.[60] In the Interim Report on the Search and Surveillance Bill the Select Committee reject the suggestion that the principles in *TVNZ* should be codified and noted that it 'is expected that these

---

59 *A Firm of Solicitors* at [82].

60 *Television New Zealand Ltd v Attorney-General* [1995] 2 NZLR 641.

general common law principles will continue to apply to media search warrants.'[61]

76. In *TVNZ v Attorney-General*, the Court was faced with a similar issue to the present case in that Police had obtained and executed a search warrant but the seized material had not yet been examined (in that case due to a Court order, s 145 of the SSA not then being in existence). The Court was required to determine whether the seizure was proper. There being no confidential informant to protect in that case, the legality of the seizure determined the matter. The Court set out some guidelines for search warrants over media organisations. It noted first that s 6 of the New Zealand Bill of Rights Act required the power in statute to issue a warrant to be interpreted consistently with s 21 of the Bill of Rights as much as possible and the search itself to be executed reasonably.[62]

77. The Court in *TVNZ* laid out some broad guidelines for the grant of a warrant over a media organisation as follows:

77.1 A warrant should not be obtained for trivial or truly minor offences (an offence of disorderly behaviour was not trivial on the facts).

77.2 As far as practicable, a warrant should not be granted or executed in a way that impairs the public dissemination of news.

77.3 It is only in "exceptional circumstances where it is truly essential in the interests of justice should a warrant be granted" if there is a substantial risk that it will lead to the "drying-up" of confidential sources for the media.

77.4 A warrant should be executed considerately and in a way that causes 'the least practicable disruption to the business of the media organisation'.

---

61 Interim Report on the Search and Surveillance Bill p 57

62 *TVNZ* at p 8.

77.5 A warrant should be reserved for situations when it is likely that the item or items sought "will have a direct and important place in the determination of the issues before the court".[63]

78. The applicant accepts this was not a minor offence. Police have attempted to reach a compromise with the applicant which would allow for his property to be copied and returned to him in order to restrict the impact on his work and did what they could to execute the warrant in a minimally intrusive way. If the material seized reveals the identity of the hacker, then it will certainly be important to any prosecution. The existence of the SSA regime for claiming and determining privilege lessens any risk that the warrant itself will reduce the likelihood of confidential sources coming forward. It is disclosure of the information, to be considered under s 68, which might have that result. That is discussed further in these submissions at paragraphs 60 to 63.

79. The search warrant application addressed the relevant *TVNZ* factors in that it was apparent from the warrant that the offence in question was not trivial and identity was an important issue in the investigation. The issue of minimally disrupting the applicant's work was addressed by Police in the operational order for the warrant.[64] Directions for addressing the effect on other potential informants can be made by the Judge who determines the originating application as is considered further in these submissions at paragraphs 95 and 96. Conditions on a warrant are not required as a general rule but are to be assessed on a case by case basis.[65] It is submitted that the necessary conditions here were those already imposed by the SSA, that is, to give the applicant the opportunity to claim privilege and only to seize material, not search it, until the privilege claim is resolved.

Application not misleading

80. It is said for the applicant that the application was misleading in that it failed to refer to the applicant as a journalist, rather he is described as a 'political author'. The warrant also notes that:

---

63 *TVNZ* at p 10-12.

64 Operational order, affidavit of Linda Cheesman, vol 1, commencing at p 55.

65 *Dotcom* at [194]

> On Wednesday 13 August 2014, Nicky HAGER a political author released a book named "Dirty Politics".
>
> HAGER stated in the book that the book was based on data provided to him on a 8 gigabyte storage thumb drive containing SLATER's illegally accessed private communication.

81. The conclusion of the warrant application states:

> Based on the comments made by HAGER in the media interviews outlined in this application, I believe that HAGER has met and knows the 'hacker' personally.
>
> I believe he has made regular and recent contact with the person responsible for illegally accessing SLATERS email and social media content.
>
> I believe this contact has been ongoing from the time SLATERS online accounts were illegally accessed up until and after the release of the Dirty Politics book.
>
> Based on the comments made by HAGAR in his book 'Dirty Politics' and media interviews, he is definitely aware the material was obtained illegally and has acknowledged that the hacker has committed a criminal offence.
>
> I believe based on HAGER's comment on page 12 of the Dirty Politics book, he had been in possession of the illegally accessed material provided to him on a 8 GB USB thumb drive.
>
> Even though HAGER has stated in his interviews returning the illegally accessed material, I believe HAGAR will still be in possession of material used to write the 'Dirty Politics' book to show provenance should there be future litigation against him. I further believe that even if material has been returned to the hacker that there will be evidential material available to identify the hacker held by HAGER on electronic storage devices and/or paper form.
>
> HAGER has stated that he knows the hacker personally and has been in regular communication prior to the books release. I believe based on this comment, HAGER will hold contact information for the 'hacker' and/or hold evidential material that will directly identify the 'hacker' or person purporting to be the 'hacker'.
>
> Although the nature of the communications was not specifically mentioned by HAGER in the public forum, I believe HAGER and the 'hacker' have been communicating either by cell phone, landline and/or internet based application.

82. The appendix to the warrant refers to the ability of a person being searched to claim privilege, including legal professional privilege.[66] That appendix was before the Judge.

---

[66] Search warrant, affidavit of Linda Cheesman, vol 1, commencing at p 17.

83. The applicant's submissions describe him as the country's 'preeminent investigative journalist' and *Dirty Politics* as triggering 'unprecedented media coverage' and 'intense public concern and debate'. With that background, and given the clear reference to the hacked material forming the basis of the book and the applicant as a 'political author', it is submitted that it is unreal to suggest that the application was misleading because it failed to use the particular word 'journalist'.

84. Police complied with the protections for a claim of privilege in the SSA. Police spoke to the applicant. He claimed privilege when asked by Detective Sergeant Beal if he was doing so.[67] Police had anticipated that that claim would be made and were equipped to seal and seize material without searching it and they followed that process.[68] One or two of the applicant's lawyers were present for most of the execution of the warrant.[69]

85. Reasonable grounds to believe that evidential material would be found are made out in the warrant application. It is important to keep in mind that not all of the matters set out in the affidavits filed for the applicant about the measures he claims to take to protect the anonymity of his sources were known to Police in advance of the search warrant. The applicant may now say that he takes measures to ensure secrecy[70], but of course those who hold information about the commission of a crime regularly take measures to ensure that Police do not obtain that information. It is common for Police to obtain evidence of a crime from someone who did not intend that that evidence be discovered. The warrant properly reflected the applicant's statement that he had returned material, but countered that with Police's belief that that would not be sufficient to render the warrant pointless. Further, the applicant's suggestion that because the hacker was known to have been security conscious, no material would be found at the applicant's house does not follow as a matter of logic. The applicant may well have been less aware, or less able, than the hacker.

---

67 Transcript of the recording of the search, affidavit of Linda Cheesman vol 9, at p 1613

68 Operational order, affidavit of Linda Cheesman, vol 1, commencing at p 55 and affidavit of Simon Beal at para 44.

69 Affidavit of Simon Beal at para 47.

86. What is for the Court to consider in assessing the sufficiency of the application is whether or not reasonable grounds existed at the time of the application. That does not require an assessment of everything the applicant now says was then the case, nor does it require Police to have taken the applicant's known statements before the warrant was applied for entirely at face value. As the Court of Appeal indicated in *Tranz Rail*, it is unsatisfactory for law enforcement officers to have to proceed on the basis that because material might be concealed or destroyed, a warrant will be fruitless.[71]

87. It was apparent from the material in the warrant application that the applicant knew the person who obtained Mr Slater's material, that he had had some information in electronic form on a USB stick from that person and had been in communication with them on more than one occasion. None of those matters are now said to be untrue. It was in the circumstances reasonable to believe that a search of his house might reveal evidence that demonstrated who the person he had been in communication with was. That could have been electronic communication or otherwise.

88. It is not necessary for an application for a warrant under s 6 of the SSA to show that a warrant is necessary or that other avenues have been exhausted. That distinguishes this case from *Director of the Serious Fraud Office v A Firm of Solicitors* where the statutory test for issuing a warrant under s 10 of the Serious Fraud Office Act 1990 was met only where reasonable grounds for believing that the use of an alternative procedure under the act would be 'ineffective'.[72] Similarly in *Tranz Rail,* a warrant under s 98A of the Commerce Act 1986 could be issued where it was 'necessary' to determine if certain conduct was taking place. The Court in considering that provision noted that s 6 of the Bill of Rights Act required that the provision be interpreted consistently with s 21 where possible but also in such a way as to make the legislation workable.[73] There is no requirement that other procedures be 'ineffective' before a warrant under s 6 of the SSA can issue. In any event, the Court in *Tranz Rail* was

---

70 See the affidavit of Nicolas Hager at paras 64-65

71 *Tranz Rail* at [31].

72 *A Firm of Solicitors* at [9].

73 *Tranz Rail* at [28].

considering other ways of accessing the same information, such as seeking voluntary disclosure, not other ways of establishing the identity of the suspect via entirely different means.

89. It is also said for the applicant that the warrant had a dual purpose that should have been disclosed in the warrant application in that Police apparently 'hoped' to charge the applicant. The evidence is clear that the applicant was treated as a witness. Had it become apparent that he had committed an offence, then of course consideration would have had to have been given to charging him. A dual purpose in applying for a warrant is any event permissible as long as it is a legitimate law enforcement purpose.[74]

Application not overbroad

90. The search warrant authorised Police to seize the following categories of material:

> … evidential material in respect of the offence specified above, namely:
>
> Evidential material comprising of documents in either electronic and/or paper form relating to the authoring of the 'Dirty Politics' book released on Wednesday 13 August 2014.
>
> Evidential material comprising of documents in either electronic and/or paper form relating to the illegally accessed content obtained from Cameron SLATER's email, Facebook and Twitter account.
>
> Evidential material comprising of communications with a person or persons who illegally accessed Cameron SLATER's email, Facebook and Twitter content.
>
> Evidential Material held on the internet or other web based storage system relating to the e-mail account nicky@paradise.net.nz and/or any other such e-mail accounts identified as being accessed by Nicky HAGER.
>
> Evidential material comprising of any documentation which will reveal the identity of Nicky HAGER's source whether held electronically and/or in paper form.

91. A search warrant not only provides authority for the search but also 'serves the important function of informing both the searchers and the searched of the

---

74 *R v Williams* [2007] NZCA 52 at [36].

legitimate scope of the search'.[75] It must be 'as specific as the circumstances allow'.[76]

92. It is submitted that the categories above are tailored towards material relating to *Dirty Politics*, which is where the unlawfully obtained material appears, and communication leading up to the publication. Given the applicant's admissions about his contact with his source, that is information that Police had reasonable grounds to believe they would find, even if some attempts had been made to make it difficult to do so and is information relevant to the offence. To the extent that material falling within one of the five categories is not also 'evidential material in respect of the offence specified' then it is not covered by the warrant. This limits the warrant to what is relevant to the inquiry. Accordingly, emails that would fall within the fourth category are only covered by the warrant if they are also evidential material in respect of the hacking.[77] If they relate to other matters then they are not covered by the warrant. In that way the warrant is prevented from being overbroad. Police have made it clear to the applicant that they are not interested in material he has relating in to informants other than the hacker.[78] If there is no material relating to the hacker to be found, then all of his material will be able to be returned to him.

93. The warrant here did need to be reasonably broad to be effective. Apart from the USB stick that the applicant had referred to having, it was not known what form his communications with his informant had taken, nor what notes or other material he might have. It was however reasonably believed, based on the applicant's own statements, that such communication had taken place. It is suggested that Police 'must have known that they had little hope of finding useful sources'. This is inconsistent with the sworn evidence of Police in this case.[79]

---

75 *Dotcom* at [71].

76 *Tranz Rail* at [41].

77 This is akin to the distinction made in *A Firm of Solicitors* at [79].

78 Transcript of the recording of the search, affidavit of Linda Cheesman vol 9, at p 1609.

79 Affidavit of David Lynch at para 68.

94. Police conducting the warrant were in a difficult position in that to do a more detailed search of the material in order to put aside material that was not relevant required a close examination of material over which privilege was claimed. The applicant has since declined to particularise his claim to privilege under s 147 of the SSA so that sifting process has still not taken place. If he wished to particularise his claim then the material over which privilege is not claimed could be sorted and anything irrelevant returned to him. This is the process contemplated by the majority of the Supreme Court in *Dotcom v Attorney-General*.[80]

95. As it is appropriate, the warrant specifies that some of the material sought could be in electronic form. It is evident from *Dotcom v Attorney-General* that in cases where computers are to be searched, searches will need to take place in order to establish what is relevant and what is not and this process can happen away from the site of the warrant itself.[81] That sifting process has been halted in this case by the applicant's privilege claim but a proper process for identifying what is relevant will need to be established if the respondents are successful here.

96. To the extent that there is a concern about information the applicant holds that he has obtained from confidential informants other than the hacker, any Judge who hears the originating application is able to put in place measures to ensure that that material is appropriately protected.

97. The applicant argues that the warrant should not have allowed Police to search for 'any other such email accounts identified as being accessed by Nicky Hager' and says that this was a breach of s 103(4)(k) of the SSA which provides for a search warrant to contain the following:

> if the warrant is intended to authorise a remote access search (for example, a search of a thing such as an Internet data storage facility that is not situated at a physical location) the access information that identifies the thing to be searched remotely:

---

80 *Dotcom* at [194].

81 *Dotcom* at [194].

98. The short point is that the warrant was not intended to authorise a remote access search. There is no need for Police to specify that the warrant is for a remote access search if the data that is sought will be accessible from a computer at the place that is to be physically searched. The definition of "computer system" in s 3 is wide enough to allow the capture of web-based material accessible from that computer:

> computer system—
>
> (a) means—
>
> (i) a computer; or
>
> (ii) 2 or more interconnected computers; or
>
> (iii) any communication links between computers or to remote terminals or another device; or
>
> (iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and
>
> (b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data

99. A remote access warrant would be needed if Police were to search the applicant's email accounts from elsewhere. Police were alive to that possibility but it was ultimately not done.[82]

100. It is also said that it was an overly broad application and that Police knew that. In fact this misconstrues the emails between Detective Sergeant Beal and Clifford Clark where officer Clark suggests that getting a warrant for 'any' email address accessed from the applicant's address would be too vague and the application instead refers to accounts identified as being accessed by the applicant himself. That, it is submitted, is not overly broad, and captures accounts that the applicant had the login details and passwords for.

The search itself

101. The legality of a search and its reasonableness are distinct questions. A lawful search, which would include one conducted under the terms of a properly

---

82 Affidavit of Simon Beal at para 55.

issued search warrant, can be unreasonable in rare cases.[83] A lawful search might be unreasonable for s 21 purposes if it is conducted in an unreasonable manner or in extreme cases of bad faith.[84] As set out above, it is submitted that this was a lawful search because it was conducted in reliance on a properly issued search warrant.

102. This search was conducted in a reasonable manner. The execution of a warrant over someone's home is always intrusive but the six Police staff who attended attempted to minimise the disruption as much as possible.[85] Police arrived at 7.40am and left at 6.40pm.[86] The search was lengthy, but this is explicable given the nature of what was being looked for and the protections that were put in place for the applicant's claim to privilege.[87] The applicant's daughter, who was not fully dressed when Police arrived, was able to dress in front of a female Police officer.

Alleged breaches of privilege

103. The applicant alleges a number of breaches by Police of his claim to journalistic privilege. One error on the part of Police in this regard is accepted. To the extent that a breach of privilege might make a search unreasonable,[88] it is submitted that the one admitted breach here did not have that effect.

104. The breaches alleged are an attempt to log into two email accounts, Mr Donovan and Detective Abbott photographing a document and sending it to NC3 and then an attempt by NC3 to access a URL in that document, a photograph sent by Detective Teo to Detective Constable Smith and steps taken by Detective Constable Smith as a result, the noting of details relating to a phone at the address and subsequent requests made in relation to those phone details, information recorded on Police property record sheets, and using computer settings to connect to the applicant's internet connection.

---

83 *Williams* at [24].

84 *Williams* at [24] to [35].

85 Affidavit of Simon Beal at para 48.

86 Affidavit of Simon Beal at para 42.

87 Affidavit of David Lynch at para 75.

88 *Southern Storm* at [48]. See also the recent decision of the Supreme Court in *R v Beckham* [2015] NZSC 98 at [129] where a lack of candour in the warrant application together with breaches of solicitor-client privilege, an absolute privilege, were found to make the warrant unlawful.

105. It is accepted that Detective Teo ought not to have emailed Detective Constable Smith with the photograph of an email that appeared to be authored by a person of interest to Police. Detective Constable Smith carried out open source searches on some of the terms in that email on 2 October.[89] The emails have since been deleted and no further steps have been taken as a result of what Police saw on that photograph. Investigations in relation to the information already known to Police continue.[90] Detective Teo and Detective Constable Smith's actions in that regard were regrettable, but amounted to a narrow and brief breach of the claimed privilege which Police have taken steps to confine. The actions of Detective Teo and Detective Constable Smith were in contrast to the instructions to Police assisting with the search as set out in the Operation Order.[91] None of the other matters complained of are accepted as breaches.

106. It is noted that the applicant claims that the evidence around this breach is misleading or intended to misinform the Court. Both of those allegations are unjustified and have not been (and nor will they be) put to either Detective Inspector Lynch or Detective Sergeant Beal. Detective Inspector Lynch was not present at the search and filed his affidavit before becoming aware of the breach. Detective Sergeant Beal had nothing further to add to the acknowledgement of the use of the material by Detective Teo. To make an allegation of deliberately misleading the Court, when there is no evidential foundation to suggest Police purposely withheld material to conceal a breach of privilege, is irresponsible.

107. The search warrant allowed Police to search "Evidential Material held on the internet or other web based storage system relating to the e-mail account nicky@paradise.net.nz and/or any other such e-mail accounts identified as being accessed by Nicky HAGER". Detective Abbott found a piece of paper with login details and passwords for two online email accounts. Detective Sergeant Beal formed the view that an email account that the applicant had the

---

89 Affidavit of Linda Cheesman, vol 14 at p 2306-2311.

90 Supplementary affidavit of Joseph Teo at para 2.

91 Affidavit of Linda Cheesman vol 1 at p 55.

login name and password for, fell within the scope of that warrant.[92] It is submitted that was a reasonable interpretation of the warrant and it could not have been a breach of privilege to try and access those accounts. It is not the account names that are important. Only reading and accessing on material found in the accounts could amount to a breach. In fact, Police were not able to access either account and so nothing further took place.[93] If they had been able to gain access, that material would have been seized and sealed.[94] To access the material later from another location, after the execution of the search warrant had concluded, would have required a remote access warrant. Police never applied for such a warrant.[95]

108. It is also alleged that it was a breach of privilege to use the settings of a computer at the address to connect to the applicant's internet and to take a photograph to facilitate that. It is difficult to see how the applicant could have privilege in his internet connection. Mr Donovan has deposed that it was his understanding that using the internet connection at the search was the correct process to follow under the SSA.[96] Such a step would seem to be allowed for by s 110(e) and (h) of the SSA. Mr Donovan has also deposed that he had difficulty in connecting to the internet and took a photograph to assist him in resolving that technical issue.[97]

109. The further steps taken in relation to the details of the phone seen at the address are set out in the affidavit of Detective Teo.[98] In short, Police were aware that phone data is usually deleted within six months and were concerned to secure it while legal proceedings were pending. Any material obtained would have been added to the material stored with the Court. As it happened, nothing was found.[99]

---

92 Affidavit of Simon Beal at para 55.

93 Affidavit of Ian Donovan at para 25.

94 Affidavit of Ian Donvan at para 30.2.

95 Affidavit of Simon Beal at para 55, s 110 SSA.

96 Affidavit of Ian Donovan at para 25.

97 Affidavit of Ian Donovan at para 25.4.1.

98 Affidavit of Joseph Teo at para 54.

99 Affidavit of Joseph Teo at para 54.

110. Similarly, the Police attempt to access a URL found at the scene was in order to ensure anything that might be disabled was secured by way of a remote access warrant if need be.[100] Instead, Police found that there was nothing to find in relation to that URL and took no further steps.

111. The records taken of the search that were kept on the investigation are the notes of what was seized on standard Police forms for the purpose.[101] It is said that keeping the notes unsealed on the file was a breach. It was obviously responsible of Police to take a note of what was found and to have that available in the event of a dispute. Police have assured the applicant that they have not used these very bare notes to progress the investigation.

112. Save for the admitted error on the part of Detective Teo and Detective Constable Smith, it is submitted that the breaches of privilege alleged here are steps Police took that were within the terms of the warrant and fall well short of the bad faith alleged by the applicant at 4.81. Merely seeing a name on a document or noting a password cannot, without more, amount to a breach of privilege nor an act in bad faith.

113. The applicant's claim to privilege did not require this investigation to come to an end. Police continue to investigate. However, no steps have been taken in reliance on the material over which privilege is claimed, save for those admitted above.

Other steps taken to obtain information relating to the applicant

114. It is not entirely clear how the applicant's claim in relation to information requests made for information relating to him fits into a judicial review proceeding. It appears more properly to be an ordinary civil proceeding with a claim for *Baigent* damages.

115. The applicant complains about information requests made to various agencies for information held about him. These were to banks, as well as to Trade Me, Spark, Vodafone, Air New Zealand and Jetstar. As a result, banking information was obtained. Trade Me and Vodafone declined to provide the

---

100 Email Clifford Clark to Jason Abbott in affidavit of Linda Cheesman, vol 14 at p 2253.

101 Property record sheets appended to affidavit of Linda Cheesman, vol 1 at p 40-44.

information sought in the absence of a production order. Spark confirmed that the applicant did not have a cell phone with Spark.[102] The applicant's bank provided banking information and other banks responded to say that they did not hold any information about the applicant.

116. It is said for the applicant that Police should not have claimed that their requests were exceptions to the Privacy Act 1993 such that the agencies could disclose the information sought. The requests relied on principle 11 which relevantly says:

> An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—
>
> ...
>
> (e) That non-compliance is necessary—
>
> (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
>
> (ii) For the enforcement of a law imposing a pecuniary penalty; or

117. Police were investigating an offence and requesting information on the basis that an exception to the Privacy Act applied. This was a legitimate and anticipated course of conduct under the Privacy Act.

118. It was open to the agencies to decline the requests and require a production order. The information requests were just that, requests. Some agencies declined to assist in the absence of a production order, others did not. Having supplied accurate information about the purpose of the request, Police discharged their responsibilities. The fact that information was said by Police to fall within an exemption under the Privacy Act did not mean that the agency who held the information was obliged in any way to provide it. Butler and Butler in *The New Zealand Bill of Rights Act* observe that it is difficult to establish

---

[102] Affidavit of Joseph Teo at paras 17-21.

a reasonable expectation of privacy in information that can be voluntarily disclosed.[103]

119. In any event, contrary to the applicant's argument, Police could have obtained a production order for this material.

120. A production order is available under s 72 of the SSA when:

> The conditions for making a production order are that there are reasonable grounds—
>
> (a) to suspect that an offence has been committed, or is being committed, or will be committed (being an offence in respect of which this Act or any enactment specified in column 2 of the Schedule authorises an enforcement officer to apply for a search warrant); and
>
> (b) to believe that the documents sought by the proposed order—
>
> > (i) constitute evidential material in respect of the offence; and
> >
> > (ii) are in the possession or under the control of the person against whom the order is sought, or will come into his or her possession or under his or her control while the order is in force.

121. An offence had been committed. It was apparent that the applicant's bank would have information about his financial circumstances. Police had reasonable grounds to believe that that financial information might disclose payments to the hacker. The term "evidential material" is broad. The Supreme Court of Canada considered a similar phrase in *CanadianOxy Chemicals Ltd v Canada (Attorney General)* and said at [15]:

> On a plain reading, the phrase 'evidence with respect to the commission of an offence' is a broad statement, encompassing all materials which might shed light on the circumstances of an event which appears to constitute an offence. The natural and ordinary meaning of this phrase is that anything relevant or rationally connected to the incident under investigation, the parties involved, and their potential culpability falls within the scope of the warrant.[104]

122. It is submitted that what was sought here would have fallen within that test.

---

[103] Butler and Butler in *The New Zealand Bill of Rights Act: A Commentary* (LexisNexis, Wellington, 2005) at 18.11.5.

[104] [1999] 1 SCR 743.

Conclusions

123. Apart from one regrettable breach of the claimed privilege during the execution of the search warrant, this was an ordinary and lawful exercise of Police power that had received the prior approval of a District Court Judge.

124. In response to a complaint about unlawful access to Mr Slater's computer, an investigation was commenced by Police. Various lines of inquiry were pursued and ultimately it was decided that a search warrant over the applicant's house was the next step given that he knew the hacker and had been communicating with him.

125. Police appropriately considered the possibility that the applicant might claim journalistic privilege. The District Court Judge, too, must have been aware of the applicant's journalism. Protections were in place to respect the apprehended claim of privilege, and they were used. The applicant's material has still not been searched by Police and his claim to privilege is still pending. When it is before the Court, he will be able to make the argument that on this occasion s 68 requires that his material not be disclosed. That is the proper process laid down by Parliament and Police have respected it.

Chronology

126. The first and second respondents' chronology of the key events forming part of the evidence is **annexed**.

List of authorities

127. A list of authorities is **annexed**.

8 July 2015

B J Horsley/K Laurenson
Counsel for the first and second respondents

CHRONOLOGY

Date	Event
19 August 2014	Cameron Slater complains by email to Assistant Commissioner Burgess that his computer has been hacked.
21 August 2014	AC Burgess asks for the District Mr Slater lives in to speak to him.
28 August 2014	Police arrange for a Counties Manukau Detective to speak to Mr Slater.
29 September 2014	Police decide to apply for search warrant.
30 September 2014	Application for search warrant made and granted.
2 October 2014	Search warrant executed.
17 October 2014	Originating application filed
30 October 2014	Judicial review filed

LIST OF AUTHORITIES

Statutes

Commerce Act 1986 s 98A

Contempt of Court Act 1981 (UK) s 10

Crimes Act 1961 s 249

Evidence Act 2006 s 68

New Zealand Bill of Rights Act 1990 ss 6, 14 & 21

Search and Surveillance Act 2012 ss 3, 6, 72, 103, 110 & 136 – 147 (Part 4, subpart 5)

Serious Fraud Office Act 1990 s 10

Cases

A Firm of Solicitors v District Court at Auckland [2006] 1 NZLR 586 (CA)

CanadianOxy Chemicals Ltd v Canada (Attorney General) [1999] 1 SCR 743.

Dotcom v Attorney-General [2014] NZSC 199

Evers v Attorney-General [2000] NZAR 372 (HC)

Gill v Attorney-General [2010] NZCA 468, [2011] 1 NZLR 433

Hill v Chief Constable of West Yorkshire [1988] 2 All ER 238 (HL).

Police v Campbell [2010] 1 NZLR 483 (HC)

R v Beckham [2015] NZSC 98

R v Commissioner of Police of the Metropolis, ex parte Blackburn. [1968] 1 All ER 763, [1968] 2 QB 118 (CA)

R v Williams [2007] NZCA 52, [2007] 3 NZLR 207

Slater v Blomfield [2014] NZHC 2221, [2014] 3 NZLR 835

Southern Storm Fishing v Chief Executive, Ministries of Fisheries [2015] NZCA 38, [2015] NZAR 816

Tranz Rail v Wellington District Court [2002] 3 NZLR 780 (CA)

Television New Zealand Ltd v Attorney-General [1995] 2 NZLR 641 (CA)

Text

Butler and Butler in *The New Zealand Bill of Rights Act: A Commentary* (LexisNexis, Wellington, 2005) at 18.11.5.