Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information analysis and advice for the Parliament

RESEARCH BRIEF

24 March 2006, no. 13, 2005–06, ISSN 1832-2883

revised 20 October 2006

Spy versus spy: Government control of sensitive information

From June to September 2004, government officials 'cleansed' computers which held copies of an original manuscript by former Office of National Assessments analyst Andrew Wilkie. Wilkie had agreed with the Government's instruction to remove some passages from the manuscript of the book *Axis of Deceit* after a lawyer hired to vet the book for sensitive content handed it over to the Attorney-General's Department. Recipients of the draft book allegedly consented under some pressure to have their computer hard drive 'cleansed'. This Brief examines the relevant agency powers and finds the use of consent in this incident raises several issues of concern such as bypassing the need for search or computer access warrants, restricting freedom of speech in relation to publishing and the accountability of Australia's national security officials.

Susan Harris Rimmer
Law & Bills Digest Section

The author wishes to highlight that this paper uses information as publicly reported in order to explore legal issues, without attempting to make a judgment on what actually transpired. Since the paper was originally published the Parliamentary Library has received a response from the Attorney-General, the Hon Philip Ruddock MP. The response contained factual clarifications and legal opinion regarding the incident. The paper has subsequently been revised to include key points of the response by the Attorney-General at Appendix A.

20 October 2006

Contents

Executive summary

From June to September 2004, government officials 'cleansed' computers which held copies of an original manuscript by former ONA analyst Andrew Wilkie. Wilkie had agreed with the Government's instruction to remove some passages from the manuscript of the book *Axis of Deceit* after a lawyer hired to vet the book for sensitive content handed it over to the Attorney-General's Department. Recipients of the draft book allegedly consented under some pressure to have their computer hard drive 'cleansed'. This Brief examines the relevant agency powers and finds the use of consent in this incident raises several issues of concern, such as agency officials bypassing the need for search or computer access warrants, restricting freedom of speech in relation to publishing on security issues, and the accountability of Australia's national security officials.

Introduction

This case raises several interesting issues around the legality of the incident, and broader policy concerns which arise as a consequence of the incident. Firstly, it is not clear which agency undertook the actions and under what legislative authority it acted. The media reported that the access to computers was undertaken by people identified as officials from the Attorney-General's Department. It seems that accessing the computers of private individuals on the grounds of protecting security is an operational matter that should not be undertaken by ordinary public servants.

The legal regime governing access to private computers holding information which may compromise Australia's national security is clearly covered by the *Australian Security Intelligence Organisation Act 1979* ('ASIO Act') and should be undertaken only under a search or computer access warrant. If the officials involved were in fact from ASIO, they should not be operating outside their legislative framework.[1]

Consent by parties should not allow government officials to undertake action they would not be authorised to do under warrant. It is unclear in this incident whether the participants could complain that their consent was only given under duress due to the threat of criminal prosecution or other action under the ASIO Act.[2]

Finally, there are several broader concerns that arise as a result of this incident, involving lack of certainty when publishing on matters of national security, specific concerns over computer warrants, and the accountability of the government officials involved.

Background

Andrew Wilkie is a former analyst with the Office of National Assessments ('ONA') who resigned in March 2003 over the war in Iraq. Wilkie received extensive publicity over his resignation.[3] He gave evidence to Australian and British parliamentary inquiries in June and

August 2003 into the intelligence used to justify sending troops to Iraq. Wilkie subsequently ran as an Australian Greens candidate in the Prime Minister's seat of Bennelong in the 2004 Federal election.

Wilkie wrote a book entitled *Axis of Deceit*, published by Black Inc. in July 2004, which discusses the intelligence relating to Iraq and how he felt the intelligence was politicised in Canberra, London, and Washington.

Earlier in 2004, Black Inc. had retained a university lecturer with an ONA background, David Wright-Neville, to check the manuscript for any inadvertent disclosures of national security information. He suggested several passages be deleted. Black Inc. then retained Captain Martin Toohey for a second opinion. Toohey was a Navy Reserve military lawyer, who had previously reviewed the Colonel Lance Collins allegations for the Government.[4] Morry Schwartz of Black Inc. alleges that Toohey then handed the manuscript to the Attorney-General's Department without the permission of the publisher or the author.[5]

A series of meetings between the publishers and a delegation of Attorney-General's Department and ONA staff was held and changes to the manuscript were agreed upon. Details of what was cut from the book are not able to be revealed under this written agreement, under threat of a criminal prosecution.[6] It was reported in the media that the deletions related to technical intelligence matters, some of which are in the public domain, but which would have gained credence from Wilkie's background as a former ONA official.[7]

There is disagreement over whether the cuts were political in nature. A 'Canberra official' is quoted by the *West Australian* as saying the changes did not affect the 'tenor, force, judgments or shape of the book'[8] with which the publisher appears to agree, stating that no changes of a political nature were made.[9] The Canberra official confirmed that the original book would not have risked the lives of overseas agents.[10] The publisher recently stated:

> There is no doubt that Wilkie's manuscript was political dynamite in an election year. Our concern was that the intense interest in it by the Government was likely to be politically motivated.
>
> This did not turn out to be the case. I can absolutely state that we weren't asked to make any changes of a political nature. The minor deletions were all bona fide and logical. They clearly related to legitimate security issues and we agreed to them willingly.[11]

Wilkie and Wright-Neville have each stated that the cuts were designed to intimidate Government critics.[12]

Part of the agreement between Wilkie, Black Inc. and the Government seems to have covered consent to the complete deletion of the original manuscript, meaning that any computer hard drive which had held a copy of the text needed to be 'cleansed' or deleted from the hard drive. Public details of the operation are limited, but it appears that 74 computers were involved.[13] The computers in the Melbourne offices of Black Inc. were worked on by a team of four government officials for five days identifying and deleting the relevant files. As Schwartz describes:

> A small team of computer experts was then sent to the Black Inc office to cleanse the offending material from our computers. They transferred the data to a hard disk then gave us the option of having it taken away or destroyed in front of us. We chose the second option, then watched them do it with a special little disk-breaking hammer. They graciously followed up this service with a customer satisfaction form.[14]

People who were emailed drafts of the book—including Wilkie's sister, documentary maker Carmel Travers and Professor Robert Manne—also had their hard drives cleansed around early September 2004, several months after the amended book had gone on sale.[15]

SBS current affairs programme *Dateline* alleged in the story 'Sledgehammer Politics', broadcast on 22 June 2005, that all parties concerned apparently consented to the activities, but were allegedly told that resisting a warrant was an offence carrying a five-year jail term. The program also alleges that making the computer incident public by the parties involved may have also been a crime. This is at odds with the reports that Andrew Wilkie did not agree to keep the fact that the book had been censored a secret.[16]

Carmel Travers sought legal advice about her right to privacy and was advised the Commonwealth officers were acting lawfully and if she did not comply with the request to access her computer, the officers could obtain a warrant. Travers alleges that during the cleansing operation, two of the hard drives of her computers were smashed with a crowbar.[17]

Black Inc. complained to the ACT Law Society about the conduct of Captain Toohey in handing the manuscript to the Government without consent, on the grounds that he had breached lawyer-client confidentiality.[18] The findings by the Law Society were not made public but an extract was published by Morry Schwartz. On 23 June 2005, the Law Society held in Captain Toohey's favour:

> His obligations of confidentiality were subject to the 'public welfare' exception, which permits disclosure of a confidence if non-disclosure might jeopardize national interest …
>
> On the available material, it was open for him to so conclude and it appears that he bona fide held such a belief. In those circumstances, any breach of confidence involved in disclosing the manuscript to the Attorney General's Department was justified in law.[19]

As of July 2005, Black Inc. was considering an appeal.

The legislative framework

Wilkie's potential liability

The question of what offence Wilkie could have committed by the two acts of emailing or publishing the original manuscript is unclear.

Provisions that could have been engaged if the original manuscript had been published in its original form include:

- 'Offences relating to espionage' under Part 5.2, Division 91 of the Commonwealth Criminal Code 1995. Among other things, section 91.1 requires the intent to prejudice the Commonwealth's security or defence, and that the person's act results in Commonwealth security or defence information being communicated to another country or foreign organisation. Section 91.2 provides a defence if the information is in the public domain with the authority of the Commonwealth. Intent under sub-section 5.2(3) of the Code is defined as 'if he or she means to bring it about or is aware that it will occur in the ordinary course of events'. The term 'security or defence' of a country is defined in section 90.1 as including 'the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies', which would appear to cover technical intelligence matters. The offence attracts a maximum penalty of a 25-year prison term. It appears unlikely that by emailing the manuscript to family and colleagues Wilkie committed an offence against section 91.1 of the Code.

- Section 70, Part VI of the *Crimes Act 1914* relating to 'Offences by and against public officers'. It is an offence under section 70 for a current or former Commonwealth officer to publish or communicate to an unauthorised person any fact or document which comes to his knowledge or possession by virtue of being a Commonwealth officer and which he or she has a duty not to disclose.[20] The maximum penalty is imprisonment for two years. It is not a strict liability offence, since relevant fault elements, such as intent and recklessness, apply.

- Part VII of the *Crimes Act 1914* relating to 'Official Secrets and Unlawful Soundings'. It is an offence under subsection 79(2) for a former Commonwealth officer to communicate 'prescribed information'[21] to any unauthorised person with the intention of prejudicing the security or defence of the Commonwealth. Intent can be inferred from conduct or known character under subsection 79(7). This offence carries a maximum seven-year jail term. It is an offence under subsection 79(3) to communicate prescribed information to an unauthorised person, which carries a maximum two year jail term.

- Section 73A of the *Defence Act 1903* relating to 'unlawfully giving or obtaining information as to defences'. It is an offence for a person who is a member of the Defence Force or a person appointed or engaged under the *Public Service Act 1999* to communicate to any other person any plan, document, or information relating to any 'fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air force aerodrome or establishment or any other naval, military or air force information' if the communication is not in the course of that person's official duty. The penalty set out in section 73F, if the offence is prosecuted summarily, is a fine not exceeding $200 or imprisonment for six months or both, or if the offence is prosecuted upon indictment, a fine of any amount or imprisonment for any term, or both.

It is not clear on the public information available that there would be a prima facie case against Wilkie under any of these sections. Presumably, if there had been, a police investigation would have been mounted. However, an offence under these sections is not a prerequisite for a warrant to be issued.

Basis of Government response

The identity of the government officials who carried out the cleansing operation and the legislative bases for their actions is unclear. For example, Australian Security Intelligence Organisation ('ASIO') officers acting under warrant are generally accompanied to operations by police officers. There was no participation by the Australian Federal Police in any reports of the incident. Government officials did not need to establish a prima facie case for a warrant to delete the manuscript from computers because all parties to the matter consented. This raises some important issues.

Some news reporters note the officials were identified as being from the Attorney-General's Department but assume that is 'shorthand for ASIO'.[22] The names of ASIO officers are protected under section 92 of the ASIO Act. As the relevant officers were not acting under warrant, confusion arose in the public arena as to which organ of the Commonwealth was acting.[23]

This is problematic for three reasons. Firstly, confusion over the identity of the officers makes it difficult to assess under what legal authority they were acting. Even with consent of the parties, the actions of Commonwealth officers must have a legal basis. Secondly, the two agencies have markedly different powers and accountability mechanisms. Thirdly, the identity of the officers determines which complaint mechanism may be accessed by the affected parties.

This brief examines two scenarios - that the officials were Attorney-General's Department public servants, and alternatively that the officials were ASIO staff acting outside the usual warrant regime.

Attorney-General's Department powers

The power for government officials (as opposed to police) to access computers is set out clearly in the relevant legislation, such as the ASIO Act or the Customs Act. The strong argument would be that Attorney-General's Department officials were outside the boundaries of their duties if accessing the computers of Australian citizens without a legislative basis for their actions, regardless of any consent given.

Under the Constitution, the Governor-General, on the advice of the Prime Minister, appoints Ministers, establishes Departments of State and formally allocates executive responsibility among Ministers through the Administrative Arrangements Order (AAO).

The AAO is published in the Commonwealth Gazette. It sets out the matters dealt with by each Department of State and the legislation administered by a Minister of State administering a Department. The AAO entry for each Department of State covers the principal matters and legislation administered by all agencies (including statutory agencies and executive agencies) within the relevant portfolio.

The Administrative Arrangements Order for the Attorney-General's Department authorises the Department to deal with 'national security, protective security policy and co-ordination'.[24]

The Attorney-General's Department website states:

> The Attorney-General's Department serves the people of Australia by providing essential expert support to the Government in the maintenance and improvement of Australia's system of law and justice.
>
> The Department is the central policy and coordinating element of the portfolio, for which the Attorney-General and Minister for Justice and Customs are responsible.[25]

Section 13 of the *Public Service Act 1999* states that, as part of the *APS Code of Conduct,* an APS employee when acting in the course of APS employment, must comply with all applicable Australian laws.

The public expectation regarding Attorney-General's Department officials would be that they provide policy advice and coordination, but do not undertake operational activities relating to national security issues in the domestic sphere. These activities have been legislated as the domain of a specific agency, namely ASIO. The activity of accessing the computers of private Australian citizens on this basis has been designated by the Australian Parliament as an act which requires a warrant. In other words, there would appear to be no legal authority for public servants in the Attorney-General's Department to undertake such an activity.

Australian Security Intelligence Organisation powers

The Attorney-General is empowered to administer the ASIO Act. The functions of ASIO are set out in section 17 of the ASIO Act, and include the function 'to obtain, correlate and evaluate intelligence relevant to security'.

The ASIO website summarises these functions as follows:

> ASIO's main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security. The ASIO Act defines 'security' as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system, and acts of foreign interference.[26]

If the officials were ASIO staff, two hypothetical questions arise:

- whether ASIO can delete data from a computer even with consent; and
- whether they could have obtained a search or computer access warrant under sections 25(5) or 25A of the ASIO Act.

Warrant regime

The test for a general search warrant under the ASIO Act is if the Minister is satisfied that there are reasonable grounds for believing that access by the Organisation to records or other things on particular premises will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security (subsection 25(2).

Under the general search warrant power contained in paragraph 25(4)(d), ASIO can remove and retain records for the purposes of making copies or inspecting the records.

Under subsection 25(5), if the Minister considers it appropriate in the circumstances, he or she can specify in a warrant any of the following things:

> (a) where there is reasonable cause to believe that data relevant to the security matter may be accessible by using a computer or other electronic equipment found on the subject premises—using the computer or other electronic equipment for the purpose of obtaining access to any such data and, if necessary to achieve that purpose, adding, deleting or altering other data in the computer or other electronic equipment;
>
> (b) using the computer or other electronic equipment to do any of the following:
>
> (i) inspecting and examining any data to which access has been obtained;
>
> (ii) converting any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, into documentary form and removing any such document;
>
> (iii) copying any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, to a storage device and removing the storage device;
>
> (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
>
> (d) any other thing reasonably incidental to any of the above. (Emphasis added)

Paragraph 25(5)(a) enables data to be deleted only for the purpose of accessing the computer. Under subsection 25(6), these warrants will not authorise:

> the addition, deletion or alteration of data, or the doing of any thing, that interferes with, interrupts or obstructs the lawful use of the computer or other electronic equipment by other persons, or that causes any loss or damage to other persons lawfully using the computer or other electronic equipment.

It is unclear what would constitute an unlawful use of the computer which would merit the deletion of data, and at what point in the process the lawfulness of the conduct would be

assessed. As the functions of ASIO relate to the purpose of obtaining, correlating and evaluating intelligence relevant to security as set out in section 17 of the ASIO Act, it is not clear that this function also includes the destruction of such information.

Under paragraph 25(7)(a) a search warrant must authorise the use of any force that is necessary and reasonable to do the things specified in the warrant.

The specific computer access warrant in section 25A of the ASIO Act enables ASIO to gain remote access to computers and is framed in similar terms to section 25:

> The Minister is only to issue the warrant if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a particular computer (the *target* computer) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the *security matter*) that is important in relation to security.

The Minister can authorise in the computer access warrant a range of things appropriate to the circumstance of the case under subsection 25A(4):

> (a) using:
> (i) a computer; or
> (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
> (iii) any other electronic equipment;
> for the purpose of obtaining access to data that is relevant to the security matter and is stored in the target computer and, if necessary to achieve that purpose, adding, deleting or altering other data in the target computer;
> (b) copying any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;
> (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
> (d) any other thing reasonably incidental to any of the above.

Again, subsection 25A(5) states that these warrants do not authorise the addition, deletion or alteration of data, or the doing of any thing, that interferes with, interrupts or obstructs the lawful use of the target computer by other persons, or that causes any loss or damage to other persons lawfully using the target computer.

The incidental power under paragraph 25(5)(d) would also not seem to authorise the destruction of the hard drive of a computer as Carmel Travers alleged.

Refusal of warrant

According to SBS TV's *Dateline*, if a warrant had been obtained, refusing to comply with the warrant would carry a five-year penalty, and disclosing anything about the computer searches would also attract a five-year penalty.[27] The Part III amendments to the ASIO Act relating to anti-terrorism passed in 2003 did create an offence carrying a five-year penalty under section

34VAA, which requires a person not to disclose any details about the warrant or operation.[28] Further, under subsection 34G(6) of the ASIO Act, a person must produce 'any record or thing' requested in accordance with the warrant. Refusal to comply carries a penalty of five years imprisonment.

However, these sections only apply to warrants obtained under section 34D, that is, warrants allowing a person to be taken in for questioning or detention under the new terrorism powers in Part III, Division 3. The secrecy requirements were reported in a confusing manner regarding the ASIO raids in June 2005.[29] Attorney-General Ruddock clarified the secrecy provisions as not relating to ordinary search warrants, leaving the people affected by the raids free to speak publicly.[30] As Waleed Aly, Melbourne lawyer and member of the Islamic Council of Victoria executive later pointed out in response to Ruddock's June 2005 statement:

> I believe Ruddock is telling the truth. But the problem is that if he isn't, we would have no way of knowing.[31]

There are no such secrecy provisions in relation to the ordinary search or computer access warrant powers. Paragraphs 25(5)(c) and 25A(4)(c) both contain the ambiguous phrase that ASIO can do 'any thing reasonably necessary to conceal the fact that any thing has been done under the warrant'. However, the *Explanatory Memorandum* for the *Australian Security Intelligence Organisation Legislation Amendment Bill 1999* seems to confirm that this wording relates to technical issues, not imposing secrecy obligations on the person concerned:

> The computer provisions permit the Minister to authorise ASIO to add, delete or alter data for the purpose of gaining access to data in a target computer and to do things that are reasonably necessary to conceal that any thing has been done under the warrant. This would include modifying access control and encryption systems.[32]

The proper interpretation of this wording has not yet been determined by a court.

The questions that therefore arise if the officials were ASIO agents are: what if the primary action by Wilkie would not have been able to sustain the granting of a warrant in the first place? What if the computer owners involved only gave their consent under duress at the threat of a criminal prosecution or other action under the ASIO Act that was not in fact justified?

Potential issues

There are several issues that arise as a result of this incident, involving freedom of speech, specific concerns over computer warrants, and the accountability of the government officials involved.

Legal privilege

The implications of the Toohey finding of lawyer-client privilege require urgent clarification. This might prove difficult for publishers to 'legal' books which contain controversial material about intelligence issues, especially if lawyers can avail themselves of the public-welfare exception to client privilege by handing manuscripts straight to the Government.

Dr David Neal of the Victorian Bar Society told *Dateline*:

> The great difficulty is that if lawyers breach that confidence, that if lawyers, either individually or as a group, show that they can't be trusted to retain confidential information, then people who are wanting to find out whether they can lawfully do something, might be inhibited from doing that and they might just simply take their chances.[33]

Or as publisher Morry Schwartz expressed it:

> What is a publisher to do if there is a possible breach of national security in a manuscript? Does he go straight to the Attorney General? This doesn't feel right. It opens the gates of unfettered power to Government, diminishing open society. So to whom do we go?[34]

He urges the Government and the Law Council of Australia to nominate a list of independent experts that could negotiate between the intelligence agencies and publishers.

Freedom of speech

The converse is also a concern: that legitimate analysis and information relating to security issues might be self-censored by authors or publishers. Admittedly, Wilkie is an unusual case, in the sense that he is an ex-ONA official writing about the issue he resigned over, but the implications for ex-public servants, academics and analysts could be wider. The implied right of political communication under the Constitution as laid down by the High Court could also potentially be infringed.[35]

Some of these fundamental issues were revisited in a different context when Major Clinton Fernandes complained in October 2005 that the Army inappropriately invoked national security laws against him to prevent the publication of his thesis on East Timor because it was critical of Government policy.[36] The book was published under the title *Reluctant Saviour* in October 2004.

Whether it is a fair assessment or not, it is clear that at least two of the affected persons in the Wilkie case viewed the Government's actions as intimidatory, even though the publisher felt the textual amendments to the draft book were fair. Wilkie's response was:

> I think a lot of it was just theatre meant to put pressure on people, almost to bully them. I think it was intended to send a very clear signal to the media, to the publishing industry, to me that they needed to be very, very careful about criticising the Government.

> I think the Government's behaviour was intended very clearly to send a signal to my former colleagues that, you know, you don't cross them, you don't resign, you don't speak out.[37]

Computer access warrant concerns

There are also privacy concerns, specific to computer access warrants, which will not be allayed by this incident. Prior to the commencement of the new search warrant provisions concerning computers (sections 25 and 25A), the Australian Privacy Charter Council noted its concerns to the Joint Committee on ASIO in 1999:

> However well intentioned, empowering ASIO to add, delete or alter data, and to modify access control and encryption systems (even if technically feasible) fatally undermines this trust and confidence. It is difficult to see how the supposed limitations on this power—not obstructing lawful use or causing loss or damage—would work in practice, and in any case they would not restore the confidence which, once lost, is gone forever.[38]

The Joint Committee report noted at paragraph 3.51 that the submission by the Attorney-General's Department in relation to the computer access amendments emphasised:

> that 'in gaining entry to a target computer ASIO is not permitted to cause damage to either computer or data.'
>
> It went on to make the point that it would, in fact, be:
>
> … in ASIO's interests to go to extreme lengths to ensure that it did not cause damage that might compromise its operations.[39]

What none of the submissions in 1999 envisaged was Commonwealth officials, ASIO or otherwise, accessing the computers of private citizens obtained by consent under threat of other legal action.

Accountability of government officials

It is unclear whether citizens are adequately informed and protected by ordinary accountability mechanisms when officials from the Attorney-General's Department or ASIO act outside the warrant regime under a consensual arrangement, but exceed their own legislated powers or appropriate conduct whilst doing so.

The subject of possible complaints based on the publicly available information could include any damage to the computers during the cleansing process, particularly that sustained by being hit with a crowbar, and potentially the behaviour reported by Carmel Travers as 'bullying'.[40]

What is less clear is whether the participants could complain that their consent was only given under duress due to the threat of criminal prosecution. The officials may have acted beyond lawful authority if the action by Wilkie would not have been able to sustain the granting of a warrant.[41]

There is no publicly available information regarding whether any of the people who had their computers accessed made a complaint. If the officials were from ASIO, there is a complaint mechanism to the Inspector-General of Intelligence and Security ('IGIS'). The IGIS has the power under the *Inspector-General of Intelligence and Security Act 1986* to take complaints from the public or initiate an inquiry of his or her own motion. The IGIS can also recommend in a report to the relevant agency that compensation is required if a person has been 'adversely affected' by action taken by an agency under section 22(2). The IGIS Annual Report 2003–04 notes that a complaint about a computer damaged after it was seized by ASIO under a search warrant was successful, and compensation was paid by ASIO in July 2003.

The accountability regime for ASIO departs from other organs of government, in that:

- decisions are exempt from the *Administrative Decisions (Judicial Review) Act 1977* (including decisions by the Minister to grant warrants targeting individuals for search or surveillance)
- the *Freedom of Information Act 1982* does not apply to an agency in relation to documents which originated with ASIO, and ASIO itself is an exempt organisation for the purposes of that Act
- human rights complaints about ASIO cannot be investigated by the Human Rights and Equal Opportunity Commission - discrimination complaints are re-directed to the IGIS; and
- ASIO is legislatively exempt from the requirements to handle personal information in accordance with the *Privacy Act 1988*.[42]

If the officials were from the Attorney-General's Department, all these avenues above would apply, and a complaint could be made to the Commonwealth Ombudsman.

From a security point of view, if the information was a potential breach of the Crimes Act or Criminal Code Act, it is curious why the cleansing occurred three months after the agreement between the publisher, author and the Commonwealth to edit parts of the book.[43]

The more fundamental problem is that if citizens feel forced to consent to activities under threat of warrants and penalties, this raises the issue of duress.[44] It means that the relevant government agency need never prove that a prima facie offence had been committed or that the original test was made out under the ASIO Act in order to obtain the relevant warrant. Any caveats or limitations that may have been placed on the relevant warrant are avoided. The warrant regime also allows for some data to be reported to the IGIS and the Joint Committee on Intelligence and Security. Travers reported that an officer 'boasted' to her that he had wiped computers 70 to 73 times.[45] An interesting question is how these activities would be recorded by the Commonwealth agencies if at all.

One interpretation of the incident is that an unintended effect of the new terrorism powers is that even when it is not an ASIO operation or ASIO is not acting under the powers, it has created uncertainty and trepidation about what the Commonwealth can do in relation to national security issues and what people can say publicly about it. It is interesting that despite the high-profile, vocal people concerned, such as Wilkie, Carmel Travers and Robert Manne, there was very little media reporting on the issue. In fact, most media reporting was in June 2005, when Travers' documentary on Iraq intelligence aired, rather than in September 2004 when the events took place.[46]

Conclusion

This paper has examined legal issues that arise from accessing the computers of private individuals, even with consent. The examination suggests that it may be preferable that any action of this nature is undertaken by the agency which has properly conferred legislative authority, and is done under warrant.[47]

Appendix A

Response by Attorney-General

The Attorney-General has advised the Parliamentary Library that:

> "…[n]o ASIO officers were involved in the computer cleansing activity".
>
> "The facts of this matter are that the Commonwealth took appropriate and lawful action to protect Australia's national security. Upon receiving a draft manuscript of Mr Wilkie's book, The Commonwealth sought expert advice from relevant agencies which indicated that certain parts of the manuscript was likely to prejudice Australia's national security. The Commonwealth considered that publication would also be in breach of legal, equitable and statutory duties of confidence owed by Mr Wilkie to the Commonwealth. Having obtained legal advice as to the options open to it (including by way of legal proceedings), the Commonwealth then negotiated, in a professional and appropriate way, with the relevant parties regarding certain aspects of the manuscript. As noted in the Brief, the publisher has publicly acknowledged that a small number of deletions agreed to during this process were bona fide and logical and clearly related to legitimate security issues.
>
> By prior arrangement, steps were taken to fully safeguard the personal information, property and privacy of the individuals involved. Importantly, no person's computer hard drive was damaged or destroyed, nor did anybody have any of their personal information taken or destroyed. Commonwealth officers only removed sensitive national security information from computers. Commonwealth-supplied hardware used to back-up information (to guard against accidental loss of information during the process) was then destroyed or erased following the completion of the process in the individual's presence so they could be sure that the Commonwealth did not retain any of their personal material. The visit by all Commonwealth officers to all premises for the purposes of removing sensitive security information occurred by prior arrangement and at a mutually agreed time and place.
>
> …
>
> One of the key suggested propositions [of the Research Brief] is that consent should not allow government officials to undertake actions that they would not otherwise be authorised to do under warrant (that is, compulsorily). This is quite ridiculous and manifestly wrong at law. People lawfully consent all the time to the taking of executive action even though the executive might not be able to take such action pursuant to the executive powers of compulsion. For example, people consent to supplying information even though there may not be a power to compel.
>
> Another suggested proposition is that consent in this case may have been vitiated by duress. During discussions on this matter, persons were notified that if they did not agree to the course of action proposed by the Commonwealth, proceedings would be commenced in the Federal Court to obtain orders to protect the Commonwealth's legitimate interests. It is quite wrong to suggest that notification of the possible vindication of legal rights by civil action amounts to duress. Indeed, forewarning relevant persons of the Commonwealth's intention to institute legal proceedings (if the matter could not be resolved by agreement) was entirely

> consonant with the Commonwealth's obligations to act as a model litigant. In the particular circumstances the Federal Court would have expected the Commonwealth to give such notice (rather than proceed ex parte) and giving notice enabled those concerned to make an informed decision as to whether to cooperate or not. I note that those most closely involved in the publication of the manuscript and the subsequent media coverage given to the Commonwealth's actions were legally represented in their dealings with the Commonwealth."

Endnotes

1. Note the clarification on this point provided by the Attorney-General at Appendix A.
2. Note the opinion provided by the Attorney-General on this point in Appendix A.
3. See L. Oakes, 'The Insider', *The Bulletin with Newsweek*, v. 121 (6364), 18 March 2003, pp. 22–24.
4. In April 2004, Colonel Lance Collins made allegations to the Prime Minister that an undue influence of the pro-Jakarta lobby had endangered Australia's national security in relation to East Timor. His concerns centred around three issues: the diligence with which some Australian officials attended to Indonesian foreign policy aims during the East Timor crisis, the conduct of the Mervyn Jenkins case, and the performance of the strategic intelligence system during the East Timor crisis. See further: Peter Cronau, 'Intelligence Wars: Behind the Lance Collins Affair', *Background Briefing*, ABC Radio National, 30 May 2004.
5. See generally M. Schwartz, 'Commentary: Black Inc. and the Attorney-General', *Australian Book Review*, August 2004, p. 8.
6. T. Cookes, 'Sledgehammer Politics', *Dateline*, SBS TV, 22 June 2005. Transcript online: http://news.sbs.com.au/dateline/, accessed on 29 June 2005.
7. B. Toohey, 'Censors go easy on spy book', *West Australian*, 14 June 2004, p. 15.
8. ibid.
9. Schwartz, loc. cit.
10. Toohey, loc. cit.
11. M. Schwartz, 'A Balancing Act: The rightful place of defamation law in open society', 2005 Redmond Barry Lecture, State Library of Victoria, 5 July 2005.
12. Cookes, op. cit.
13. P. Kalina, 'Truth falls to Iraq war of lies', *The Age*, 16 June 2005, p. 15.
14. Schwartz, 2005, loc. cit.
15. T. Cookes, 'Sledgehammer Politics', op. cit.
16. Kalina, op. cit.

17. Cookes, op. cit. Note the clarification provided by the Attorney-General on this point in Appendix A.
18. F. Shiel, 'Lawyer cleared over whistleblower book', *The Age*, 23 June 2005, p. 9.
19. Quoted in Schwartz, 2005, op. cit. ACT Law Society findings are made available only to the parties concerned.
20. The circumstances where a legal duty not to disclose might arise were recently discussed in the Federal Court case of *Bennett v President HREOC* [2003] FCA 1433. See further Ian Holland and Peter Prince, 'Public Servants Speaking Publicly: The Bennett Case', *Research Note*, no. 31, Parliamentary Library, 2003–04.
21. Section 77 of the *Crimes Act 1914* defines 'information' means information of any kind whatsoever, whether true or false and whether in a material form or not, and includes: (a) an opinion; and (b) a report of a conversation.
22. J. Coxsedge, 'Truth, Lies and Intelligence', *The Guardian*, 29 June 2005, http://www.cpa.org.au/garchve05/1234coxsedge.html accessed 4 July 2005.
23. Note the clarification provided by the Attorney-General on this point in Appendix A.
24. Administrative Arrangements Order, 16 December 2004.
25. www.ag.gov.au, accessed 15 February 2006.
26. www.asio.gov.au, accessed 15 February 2006.
27. Cookes, op. cit.
28. *ASIO Legislation Amendment Act 2003*.
29. I. Munro, 'ASIO should lose some powers says Fraser', *The Age*, 29 June 2005, p. 7. See further SBS TV *Dateline* interview with Rob Stary, 29 June 2005.
30. W. Aly, 'ASIO raids risk eroding our trust in justice,' *The Age*, 1 July 2005, p. 15.
31. ibid.
32. *Explanatory Memorandum, Australian Security Intelligence Organisation Legislation Amendment Bill 1999*, Bill No. 99051, 24 March 1999, p. 8.
33. Cookes, op. cit.
34. Schwartz, 2005, op. cit.
35. Mason CJ described the freedom of political communication as follows in the High Court decision *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, at 138.

> The point is that the representatives who are members of Parliament and Ministers of State are not only chosen by the people but exercise their legislative and executive powers as representatives of the people. And in the exercise of those powers the representatives of necessity are accountable to the people for what they do and have a responsibility to take account of the views of the people on whose behalf they act... Indispensable to that accountability and that responsibility is freedom of communication, at least in relation to public affairs and political discussion. Only by exercising that

> freedom can the citizen communicate his or her views on the wide range of matters that may call for, or are relevant to, political action or decision. Only by exercising that freedom can the citizen criticise government decisions and actions, seek to bring about change, call for action where none has been taken and in this way influence the elected representatives.

36. Eleanor Hall, 'The World Today', *ABC Radio*, 13 October 2005.
37. Cookes, op. cit.
38. Australian Privacy Charter Council, Submission to the Parliamentary Joint Committee on the Australian Security Intelligence Organization, Inquiry into the Australian Security Intelligence Organisation Legislation Amendment Bill 1999, *Submission No. 11*, p. 4.
39. Attorney-General, Submission to the Parliamentary Joint Committee on the Australian Security Intelligence Organization, Inquiry into the Australian Security Intelligence Organisation Legislation Amendment Bill 1999, *Submission No. 9*, p. 3.
40. Kalina, op. cit.
41. Note the opinion provided by the Attorney-General on this point in Appendix A.
42. M. Head, 'ASIO, Secrecy and Lack of Accountability', *E-Law: Murdoch University Electronic Journal of Law*, vol. 11, No. 4, December 2004, http://www.murdoch.edu.au/elaw/issues/v11n4/head114nf.html, accessed on 4 July 2005.
43. D. Snow, 'Big Brother sends in the hit squads to clean up national security threat', *Sydney Morning Herald*, 18 September 2004, p. 3.
44. Note the opinion provided by the Attorney-General on this point in Appendix A.
45. Cookes, op. cit.
46. Noted by both P. Kalina, 'Truth falls to Iraq war of lies', *The Age*, 16 June 2005, p. 15, and J. Coxsedge, 'Truth, Lies and Intelligence', *The Guardian*, 29 June 2005.
47. Note the opinion provided by the Attorney-General on this point in Appendix A.
