Sal Humphreys, Melissa de Zwart
Data retention, journalist freedoms and whistleblowers
Media International Australia, 2017; 165(1):103-116

Published version available via DOI: http://dx.doi.org/10.1177/1329878X17701846

Data retention, journalist freedoms and whistleblowers

The digital networked structures of the internet and mobile communications have provided extraordinary opportunities for the opening out of debates and the creation of public spheres previously not possible, but there has also been an increase in surveillance that puts the issue of freedom of expression in question. The role of journalists in these debates remains an important one, despite the apparent democratisation of information made possible by the internet, as journalists can provide an essential conduit between news sources and the public sphere. As members of the 'fourth estate' journalists have enjoyed certain limited protections for themselves and their sources under the laws of various countries. These protections are now uniquely challenged in the context of metadata retention and enhanced surveillance and national security protections.

In the Australian context, a number of laws have been passed in the last several years that are of concern and are the focus of this paper. However, it is worth noting, by way of background, that the fourth estate has historically been constrained by the Australian regulatory context. In the first instance, the Australian media has been seen as somewhat compromised by the concentration of media ownership, which has led to a lack of diversity in coverage, and the pursuit of the particular agendas of the owners (Pusey and McCutcheon 2011:22). Murdoch, Packer and Fairfax news organisations have historically dominated the media landscape, and in recent times, cross media ownership regulations designed to preserve the already somewhat limited diversity of the Australian media landscape have been relaxed (Broadcasting Services Amendment (Media Ownership) Act 2006 and the Broadcasting Legislation Amendment (Media Reform Bill) 2016 under consideration. See also Given 2007). In addition, Australian defamation laws are much stricter than their US and UK equivalents, with high payouts to plaintiffs particularly in New South Wales, discouraging critique of public figures and suppressing robust journalism. The Crimes Act 1914 (Cth) imposes harsh penalties on Commonwealth Government employees who disclose information that they have obtained in the course of their official duties to anyone outside of those duties. Further, the Australian Government itself has even resorted to copyright laws in order to prevent publication and analysis of official documents (*Commonwealth v John Fairfax & Sons Ltd* (1980) 147 CLR 39). Thus the current raft of legislation comes on top of some already concerning constraints on media freedoms and the ability of journalists to pursue investigative and watchdog reporting.

In 2015 the Australian Federal Government passed a new data retention bill obliging ISPs to retain metadata of their customers' activities for two years and to make that metadata available to government agencies under what some would say are very lax conditions. The warrantless access to citizens' internet and phone metadata is mitigated in the case of journalists. Here the government has introduced some curious warrant mechanisms that purport to act as a check on the power of the security agencies. At risk is the journalists' ability to assure confidentiality to their sources as, when security agencies access their metadata they can, through evidence or inference, identify journalists' contact with whistleblowers. Further legislation under the Australian Security Intelligence Organisation (ASIO) Act criminalises the journalist who publishes any material relating to 'Special Intelligence Operations' with a threat of 5 -10 years imprisonment. Other laws constrain professionals (such as doctors and counsellors) from speaking out about conditions in off-shore detention centres for asylum seekers (Border Force Act). Whistleblower laws offer the very narrowest of protections and essentially criminalise most whistleblower actions, whether they prove to be in the public interest or not.

This paper will explore the new legislation affecting journalists, journalists' responses to it, as well as considering the implications in the broader context of discourses of national security. The 'necessary' trade-offs between democratic freedoms and safety suggested by these discourses indicate a growing willingness of the Australian government to incrementally assign itself more power with less accountability in the name of national security. The paper will consider the position of the mainstream media in relation to government, but also in relation to the increasingly complex world of networked journalism, where non-institutional actors play a role in revealing what the mainstream media may choose to, or be forced to, suppress. It is observed that some of these developments are out of step with developments in other jurisdictions with respect to retention and access to metadata, such as in the EU under the European Court of Justice's 2014 declaration regarding the invalidity of the Data Protection Directive of 2006. Even the US may have greater checks and balances upon the operation of equivalent laws, with the role of the First and Fourth Amendments. No such protections or limitations apply under Australian Constitutional Law. In Australia there is only an implied freedom of communication concerning government and political matters (*Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520).

If we consider that the government, corporations, the media and citizens each have a certain power to scrutinise the others, we can see that when these abilities to scrutinise and be subject to scrutiny are held in balance, it can result in a functioning democracy – each arm playing a role in holding the others accountable for their actions. However, the health of the democracy is at risk if this dynamically held tension goes out of balance. When government increases surveillance of its citizens and at the same time reduces its own accountability through making more of its workings secret there is cause for concern. Add to this that the government increasingly relies on partnerships with corporations to gather data and to carry out its surveillance activities and the balance can seem even further out of alignment. What role can the press and non-institutional actors and citizens take in the face of this insidious creep towards a lack of transparency? We acknowledge the importance of public spheres and conversations generated through social media platforms but the role of algorithmically created news feeds in social media, and the responsibility of platforms as media organisations requires a separate paper.

The Laws

There have been a number of different pieces of legislation passed in Australia over the last few years that have added to the government's power to scrutinise the population and cloak its activities in secrecy. These include the metadata retention laws passed in 2015, section 35P of the ASIO Act, the Border Force Act, and some very restrictive whistleblower legislation (which could not be dignified with the term 'protection'). These will be briefly canvassed below to give a sense of the general legal context in which journalists are acting.

The meta data retention law enacted by the Australian Commonwealth Government, (Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015) requires Telecommunications Providers to retain customer metadata for two years for law enforcement and security purposes. It enables warrantless access to this metadata for a range of government agencies (21 in all). The metadata does not include the content of communications but, as has been pointed out numerous times, the information contained in metadata is rich enough to be the basis of securing convictions of whistleblowers and is even the basis on which the US kills people (with drone strikes for instance) as asserted by the former head of the NSA and CIA Michael Hayden (Cole et al., 2014. See also Scahill, 2016). Metadata includes telephone numbers called and received from, the

time and length of calls, the location of the parties making calls, the IP addresses of computers from which messages are received or sent, email addresses of messages (to and from), various chat site data, the location of individuals involved in the communications and the names of applications used, and so on.

The government has been at pains to employ a discourse which insists that, because the content of communication is not looked at, there is nothing for citizens to worry about. Metadata collection, they argue, is not an invasion of privacy and can't tell them much at all. Disclaimers of the, by now rather tired "if you've got nothing to hide you've got nothing to fear" variety, belie the level of information contained in metadata and the *inferences* that are routinely made from it. Metadata is in fact a messy, opaque and invisible layer of data we give off in our communications (Ganesh and Hankey, 2015). It is used in equally opaque fashion by both corporations and governments. It is hard to understand what levels of privacy Australians can achieve in the face of metadata collection. Malcolm Turnbull, the Australian Prime Minister who several years earlier, while his party was in opposition, had advocated strongly against metadata retention laws (Turnbull, 2012), suggesting they were an incursion into peoples' privacy and an "attempt to restrain free speech", oversaw the passing and implementation of the new laws once he was in government. He also suggested, in a confusingly contradictory way, that people should be encrypting their communications anyway, as he does himself (Grubb, 2015). Ultimately the bipartisan support for the metadata retention laws suggests that there will be few changes in the near future to this new set of powers taken by the government and its policing and security agencies. Of concern in this paper is the way in which it jeopardises the ability of journalists to maintain the confidentiality of their sources.

This issue was the minor controversy that (briefly) held up the passage of the new law. An amendment was accepted that created a warrant process for accessing journalists' metadata. Under these provisions, agencies are prohibited from authorising the disclosure of journalists' or their employers' telecommunications data for the purposes of identifying a "source" without a Journalist Information Warrant. This Journalist Information Warrant however, is a curious, secretive and probably ineffective process if a journalist is concerned about protecting sources. A warrant can be sought by any one of 21 government agencies, by application to an "Issuing Authority", an appointment from judges of the Federal Court or Administrative Appeals Tribunal (or to the Attorney-General in the case of ASIO) who must be satisfied that the 'public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source' having regard to a number of factors. The journalist is never told about the application and cannot speak to the court on his or her own behalf as to why the application should not be granted. Instead the Prime Minister appoints a "Public Interest Advocate" who speaks on behalf of the public interest. These government appointed advocates (currently two former judges) are under no obligation to champion the journalist's position, and may never take the point of view of the journalist or advocate on their behalf. We will never know, because the process is held in secret and anyone revealing the existence of the warrant application or the result of it faces penalties of up to 2 years imprisonment. In this way the journalist will never know whether their metadata has been accessed by security agencies and nor will we. The take home message is that any source who has contacted a journalist electronically either by phone or internet, without stringent encryption measures which encrypt metadata (a difficult process requiring some skill and effort) will not be guaranteed confidentiality. If they met in a café and had their phones with them, they can be linked through GPS metadata. If there was any email contact or phone contact, they are compromised. This regime is added to a system which is already known to be somewhat leaky, with data being accessed for illegal purposes in various government agencies over time. The addition of so much more data available to so many agencies is troubling.

Section 35P of the ASIO Act, a further piece of legislation introduced in 2014 criminalises the act of reporting on any Special Intelligence Operation (SIO) being carried out by ASIO. A 'Special Intelligence Operation' is an operation in relation to which a special intelligence operation authority has been granted. It is carried out for a purpose relevant to the performance of one or more special intelligence functions (s 4). Special Intelligence Operations are authorized illegal actions carried out by ASIO. They grant broad immunities with respect to criminal liability for agents' conduct during the operations. They are secret operations and s35P makes it a crime to disclose any information relating to an SIO, now or in the future, anywhere, even if the information is currently already in the public domain. As ASIO consistently refuses to comment on any "Operational Matters", and as the SIOs are secret, it is almost impossible to know whether information a journalist wishes to publish is in fact part of an SIO. This creates a great deal of uncertainty, as is pointed out in the Gyles Report of 2015. This report, commissioned by the Prime Minister from the Independent National Security Legislation Monitor to assess the impact of section 35P on journalist freedoms, criticizes the section on a number of fronts.

Gyles suggests there are two areas of concern. Firstly that the uncertainty as to what may be published about ASIO creates a chilling effect that is detrimental to the constitutionally implied right to freedom of communication. Secondly the provision prohibits the disclosure of information, "regardless of whether it has any, or continuing, operational significance and even if it discloses reprehensible conduct by ASIO insiders."(Gyles, 2015). The report suggested a number of changes be made to the Act and the government agreed in February 2016 to implement the recommendations of the Gyles Report, but has yet to do so. The changes create a number of more nuanced distinctions between 'insiders' to ASIO and 'outsiders' (meaning journalists) and make for slightly less uncertainty around what may be published. Another recommendation is that publication can take place if the information is already in the public domain (however it seems that the first to put it in the public domain can still be punished) and also that inadvertent disclosure when not aware of the SIO will not be criminalised. However the basic intent of the section – to pursue whistleblowers and deter journalists with criminal penalties remains and its intent to chill freedom of speech around ASIO and security operations and the five-ten year imprisonment penalties also remain. The journalists' union (the MEAA) is not satisfied with the outcome and suggests that it still criminalises journalists for doing their job and that "Section 35P seeks to stifle or punish legitimate public interest journalism."(Murphy, 2016)

The process of the implementation and review of s35P is a source of both optimism and pessimism. On the one hand, the review process by the independent monitor can be seen to be working, at least to some extent. On the other hand, while the government has said it will make some adjustments, the intent of s35P to criminalise both whistleblowers and the journalists they disclose to, remains a cause for concern. The recommended amendments make the legislation only slightly less concerning.

The Border Force Act 2015 (Cth) is a further piece of legislation which has a secrecy provision (section 42) which prohibits "entrusted persons" (such as doctors, counsellors, detention centre employees, etc) from revealing "protected information" (which means information that was obtained by a person in the person's capacity as an entrusted person). There is a penalty of up to 2 years imprisonment. It follows on years of policies made with bipartisan support that have seen asylum seekers held in indefinite detention despite international law obligations, and journalists denied access to the detention centres. The Border Force Act can be seen as a law aimed at closing down whistleblowers and creating a chilling effect on freedom of expression. In relation to the Australian offshore detention centres, it creates a great deal of uncertainty about what professionals

employed, either directly or through contracts with companies operating the services on behalf of the government, are able to disclose without fear of reprisal. Doctors have protested that they are obligated to report abuse under their professional standards, but have been silenced by the heavy handed approach of the Border Force Act. *The Guardian Australia* reported that doctors have had their phone records accessed and one was sacked after speaking out about conditions in the detention centres (Doherty, 2016). A group of doctors are challenging section 42 in the High Court at the time of writing.

The final area of legislation to mention in this context is the **laws pertaining to whistleblowers**. There are existing laws under the criminal code that pertain to terrorism, treason, espionage and so on. There are offences under the Crimes Act such as Section 70 which restricts disclosure of information by current and former Commonwealth officers, and the communication of official secrets, even to Members of Parliament. This was the law under which Allan Robert Kessing was convicted in 2007 after allegedly revealing information contained in his own report about corruption in the Customs Department that led to an investigation of airport security and an allocation of more than $200m to address the identified problems (Vaughn, 2012). The exposure of misconduct ultimately worked very much in the interest of national security and public safety. Kessing, it should be noted, was convicted on the basis of metadata – a phone call was made from a public phone box near his home to a media organisation (Coulthart, 2015). The fact that the government pursued Kessing and that he was convicted on the basis of metadata rather than any actual evidence of content being disclosed is a telling indication of the government's attitude to whistleblowers and metadata. Although the whistleblower may be doing exactly the right thing by revealing information vital to the public interest, the desire to discourage any whistleblower action can be seen to motivate government actions.

The Public Interest Disclosure Act 2013 (Cth) which is intended to 'promote the integrity and accountability of the Commonwealth public sector' is the government's whistleblower 'protection' law. It is very restrictive in what it considers legitimate disclosure and includes elements such as having to disclose within the organisation first (always a problem if trying to report on corruption or misconduct of senior management within organisations) and that the person must be a current Commonwealth Government employee – often whistleblowers only feel safe to disclose information after they have left an organisation. It also defines a narrow range of issues around which disclosures can be made. It could be argued that it offers very little protection to whistleblowers and probably acts more as a discouragement than an incentive to call out misconduct and corruption. Added to this law is the patchwork of laws that exist in States and Territories as well as corporate whistleblower laws and policies, all of which serves to create confusion over the nuances of which law might apply to people wishing to expose misconduct.

Journalists' responses

A number of journalists have made public statements about the laws as they have passed, and the Journalists' union, the MEAA has made some very strongly worded protests as well. In the foreword to the MEAA report "Criminalising the truth, suppressing the right to know"(MEAA, 2016) Paul Murphy suggests

> In just a few short years, Australia has fallen from being a bastion of press freedom to a country that has passed a raft of national security laws that allow government agencies to pursue journalists and their sources and criminalises legitimate journalism in the public

> interest. Increasingly, governments are denying the public's right to know and moves are underway to deny information from becoming public. (p4)

As journalist Ross Coulthart put it "I suspect the metadata laws are part of an opportunistic push by our police and intelligence services to use the current national security crisis to try to shut the door on journalistic investigation into their activities." (Coulthart 2105 NP). Coulthart argues that the pursuit of whistleblowers in such a punitive fashion as the new laws allow often has nothing to do with national security and everything to do with the government trying to save itself from further embarrassments. Many of the whistleblower cases where public servants expose government incompetence or corruption, such as the Kessing case mentioned earlier, actually seek to expose existing public safety risks, rather than themselves constituting threats to national security. The definition of security is seemingly broad and elastic. The chilling effect seems intentional. Coulthart mentions one example of a potential whistleblower from an immigration detention centre who approached him with material evidence of young boys being raped by men in the facility. But because the source had rung him, he had to warn him that he could go to prison if traced through the metadata. The source withdrew his offer, "and that's why metadata is killing investigative journalism." (Coulthart, 2015: np)

Sydney journalist Ben Grubb made a very public case of his attempts to gain access to his own metadata from his telecommunications provider Telstra over a period of several years. His long running battle through the courts highlighted the fact that agencies such as the RSPCA (Royal Society for the Prevention of Cruelty to Animals) could access his metadata but he could not. The courts eventually held that he should be able to access at least some of his metadata (Grubb, 2014), but this was later overturned in the Court of Administrative Appeals. The arguments in this case were about whether metadata was personal information and go to the heart of privacy arguments. The appeal that Telstra won essentially discarded the initial finding that metadata, because it is used in conjunction with other streams of data constitutes personally identifiable information. In the appeal, the court overturned this by only recognizing the metadata as signals data 'about' the devices and addresses of messages, not 'about' the user. It would seem then, that despite the fact that metadata is constantly used to identify people by cross matching it with other metadata, the court would only be prepared to recognize it as signals information in isolation, rather than as information with multiple uses and functions.

The point of trying to follow these cases is that we can glean some indication about how courts might look upon future arguments around metadata. The refusal to acknowledge the functional use of metadata to identify people does not bode well for arguments that the government should not be accessing that metadata on the basis of privacy concerns. But of course journalists have a much more urgent concern about the protection of their sources. The journalist information warrants seem an ineffective measure of protection. Commentary on these warrants from Day and Molnar in *The Conversation* suggests "the current manifestation of warrant requirements for journalists in Australia's data retention scheme would actually do little to meaningfully defend press freedoms" (Day and Molnar, 2015). It is characterized as a rather easy hurdle for security agencies to circumvent and one we are not likely to know the effectiveness of. They suggest that in the US the model for security agencies accessing journalist data at least allows journalists to represent themselves and their interests in court – they know about the warrants and they are able to defend the integrity of their sources in a court. In Australia, Laurie Oakes pointed out that:

> There will be Public Interest Advocates — lawyers appointed by the government — able to contest warrant applications, but they won't be standing in the shoes of journalists or media

> organisations. In fact, the Attorney-General's Department says candidly that there will be times when the advocates will support issuing a warrant. (2016:8)

The ability of a journalist to protect their sources in the digital age is compromised on many fronts, including through metadata, GPS data, CCTV and phone data (Pearson, 2015). Journalist Jonathon Stern suggests many journalists are ill-prepared when it comes to understanding how to protect their sources in the digital age. He points out how easy it is to endanger a source by careless actions carried out in ignorance (Holmes, 2015). Understanding how metadata is captured and how the technologies of encryption work is one part of the problem. However another part of the problem is in understanding the legal territory. Here the chilling effect is probably of greatest concern. In a study done on journalists' understanding of shield laws in Australia it was found that most of the journalists surveyed were ignorant about the protections actually offered by shield laws and also that they had little idea about data retention laws or how to go about keeping sources secure (Fernandez and Pearson, 2015). In the face of this uncertainty the result is often a chilling effect on speech. The complexity of the legal territory was already a factor before the latest security laws were introduced. In considering the counter-terrorism laws in place around 2007, McNamara (2009) concluded that the legal framework was so complex that it created uncertainty that almost certainly has a chilling effect. He suggests that there is discursive deployment of risk and security by authorities which attempts to control the flow of information beyond the legal limits available to the government. Thus control is exerted in the shadow of the law. The secrecy which surrounds many of the processes makes it difficult to determine the actual direct effects of any interventions which may occur (McNamara, 2009). Ruby et al sargue that "State control via new security legislationhas been central to discouraging journalism" {Ruby, 2016 #805}

A further question that arises for journalists from the current laws is about who is actually defined as a journalist under the law. As Gyles (2016) pointed out in his report on s35P, the definition of journalist varies between a number of different legal frameworks. Some laws such as shield laws in the Evidence Act adopted a broad definition that included bloggers, tweeters, and aggregators as well as a variety of mediums of publication, although this was narrowed in an amendment in 2010. Shield laws under the Broadcasting Services Act adopt a narrower definition which restricts the category to people employed professionally by media organisations. He also points to variations between Federal and State laws. The status of freelancers and professional journalists who are self-employed remains a grey area, which Gyles doesn't attempt to clear up. Thus digital media can be seen to have ushered in not only the possibilities and risks of metadata and surveillance but also uncertainty about who actually qualifies as a journalist under the variety of laws that offer protections and punishments to journalists. The low barriers to entry for publishing online and the rise of citizen journalism practices create further uncertainty in this area.

The commercial media – balancing roles?

Laurie Oakes, a well-known senior journalist who works variously for television and newspaper outlets, gave a speech to the Melbourne Press Freedom Australia dinner in 2015 in which he addressed the issues arising from the current tranche of security laws discussed above. One of his key points was that Australian journalists essentially dropped the ball in responding in a timely fashion to the legislation. He suggests that the media have been complacent and as a result these laws have been passed with little protest from journalists (Oakes, 2016). He suggests "We were too slow to recognize the threat. Too late, and probably too polite in pushing back." (Oakes 2016:6) It is

to this issue of the level of vigor with which the press in Australia have been pursuing investigative journalism that we want to turn to now.

In the balancing act between government, corporations, the press and citizens mentioned at the start of this paper, we noted that the government is increasingly partnering with commercial organisations in matters of security and data gathering. Journalists in the commercial press face a number of dilemmas in relation to their ability to scrutinize the government and its actions. The first, as alluded to above, is that the established media institutions have become complacent about their scrutiny. Reporters often rely on friendly relationships with government bureaucrats and politicians to keep the channels of information flowing. It has been pointed out that the press are sometimes reluctant to criticize or expose the government for fear of losing access to those flows of information that they otherwise rely on (Andrejevic 2014). The complicity of the mainstream media in supporting government agendas has been commented on from a number of fronts. Matthew Rickertson (2013), who assisted in the Finkelstein report into Media integrity in Australia in 2012, asserts that "important public policy discussions were being distorted or ignored by much of the mainstream news media" (Rickertson, 2013: 150). Andrejevic (2014) similarly points to the failings of the US mainstream media in their job as watchdogs of government. He suggests there has been a "dramatic failure of conventional channels for challenging power or holding it accountable." (Andrejevic, 2014: 2624) and that "[t]he established system for challenging power has conceded its own dysfunction" (2014:2625) when both the *Washington Post* and *The New York Times* apologized for not properly investigating and reporting on the Iraq weapons of mass destruction stories that led to the US invasion of Iraq. Benkler (2011) also points to the cozy relationship between the US government and the mainstream press, and the ways in which the government partners with commercial organisations which may in turn also have strong links with media organisations. The general point being that there are a range of disincentives for mainstream commercial media to engage in critique of government policies.

Alongside this perceived complicity sits the commercial reality of many media organisations, that entertainment is more profitable than investigative news journalism. The resources that many commercial media enterprises put towards investigative journalism are decreasing. With the advertising dollar that traditionally drove the business model of news organisations rapidly fragmenting and shifting to other areas and platforms, the money available to invest in investigative reporting is shrinking. This is not to say that all journalists or mainstream media organisations are failing in this area, but there is clearly a problem that is manifesting through issues of changing media business models, and through a changing understanding of the institutional function of the media.

Part of the change in business models is derived from the increased competition from online media platforms for the advertising dollar. There is also a certain competitiveness with online journalism which is seen to be less than professional and less than credible by many mainstream press journalists. As was pointed out above, there are grey areas around who actually can claim the title of journalist in the current legal terrain, but this extends also to the more sociocultural domain of the profession. As the perception of the mainstream press as complicit with big business and government interests has taken hold, we have seen a rise in the scrutiny of the press itself from citizen journalists and a variety of non-institutional actors. The recent release of the 'Podesta emails' (a series of emails on deals involving Hillary Clinton's campaign manager John Podesta, including deals done with media reporters) by Wikileaks, although controversial, nonetheless illuminates the relationship between those in government and journalists, with the influence on what journalists publish demonstrated as profound, and the pipelines of information between politicians and

journalists also revealed in some detail (Greenwald, 2016). As Benkler (2011) points out there are good and bad practices on either side of the fence – examples of great investigative journalism emerging from both the networked fourth estate and the mainstream media, as well as some unethical, inaccurate or lazy examples. He also points to the very strong interrelationship between the networked fourth estate and the more conventional press, with much criss-crossing of stories building back and forth between media sources and platforms.

Into this mix is added the conversations of social media – the debates held through platforms such as Twitter and Facebook which may sometimes draw heavily on mainstream press stories, but also may be the generative source of waves of conversations in the public sphere. The press will often pick up on issues that have gone viral in social media, meaning that the agenda setting functions of the press have now become slightly more distributed. Those conversing via social media may not consider themselves to be citizen journalists even though the effect of the commentary carries some weight in the sphere of journalism and the public sphere. When considering the agenda setting possibilities from social media, the role of algorithms in selecting and amplifying trends must also be considered. Facebook's recent experiments in curation by people and algorithms and then by fully automating through algorithms have been interesting to say the least (Thielman, 2016).

Thus with regard to the model of society presented in the opening section of this paper, the role of the press as separate from the government and corporations and able to scrutinize each on behalf of citizens seems less plausible now. Although not a new dilemma many mainstream media organisations have become even more thoroughly commercial, less disinterested and impartial, and more part of an elite set of institutions in society that are linked rather than interrogatory. Keane (2013 np) points to the way Fairfax press in Australia and the *New York Times* in the US both suppressed leaked documents available to them, acting as gatekeepers who only reluctantly published information on the leaked cables from Wikileaks after intense pressure from other outlets who *did* publish. The *New York Times* took the cables to the US State Department to censor them first. According to Keane "The main reason the NYT allowed this was because it didn't want to cut off the supply of the classified information from insiders that the paper thrives on – US Governments are happy to reveal plenty of secret information, as long as it serves their own political interests."(Keane, 2013) He suggests this is one reason Snowden did not go to the NYT with his leaks.

Journalists who wish to pursue investigative stories may find themselves without institutional supports. The complacency highlighted by Oakes is probably no accident. Indeed Oakes points to an editorial in *The Australian* (a Murdoch daily) which suggested the new laws would have no impact on the practices of journalism and were necessary for national security (Oakes 2016:7). Some of its own reporters disagreed with this assessment, but it displays the nature of the relationship of editorial management within this powerful commercial organisation and government. The refusal to countenance debate or to ask critical questions of the policy led to a muted and insignificant debate on the issues.

Where to from here?

Investigative journalism in Australia is not dead, and the public conversation, although somewhat diminished and muted, still exists through the agency of the press in Australia, although it seems political discourse may come to rely on non-Press actors more and more. For whistleblowers the disincentives are strong, but as has recently been demonstrated, not insurmountable. *The Guardian Australia* at the time of writing, revealed information from a leak of 2000 documents from the Nauru Detention Centre. This has led to some public debate and at the time of writing further pressure on the government to change its practices around the indefinite detention and mistreatment of

refugees held on Nauru. It is too early to tell whether the government will actually respond and how much other media outlets will take up and broaden the public debate. Murdoch's News Corp has initially reported with some articles on the leaks. The fact of the leak and the publication of the articles by *The Guardian* indicate that it is still possible to call the government to account on its practices via whistleblowing and publication in the mainstream media, as well as documentaries such as *Chasing Asylum* (2016). Whether section 35P of the ASIO Act or the Border Force Act will be used to track and punish the whistleblower or the *Guardian Australia* remains to be seen, and given that reporting on this may be illegal, may never be publicly disclosed.

In this section we want to consider technological solutions to the incursions of metadata tracking, the role of the 'networked fourth estate' (Benkler 2011), the role of non-state, non-institutional actors such as Wikileaks , Anonymous and hackers more generally, as well as non-profit press outlets such as the *Guardian Australia*.

Avoiding surveillance has become a much more complex proposition in this era of near ubiquitous and interlocking systems of tracking. There is much talk of encryption, and there are sites online such as The Centre for Investigative Journalism[1] which offer manuals and tips and tools for training journalists in how to use encryption to try to secure their sources. At the very basic level, this would seem to be a minimum requirement and one which many journalists have not engaged with (Fernandez and Pearson 2015). However technological solutions run a number of risks. As the report into encryption released by the Harvard Berkman Centre (Berkman Center for Internet and Society, 2016) on the 'going dark' debates suggests, there are many areas where, because of incompatibilities and gaps in the systems used on the internet, encryption is subject to failure. Metadata, by its very nature (as signals data for the transmission of content) does not lend itself to encryption. The process of masking metadata can fall apart at points of entry and exit into systems of masking. Looking at a more political angle of encryption, 2016 also saw Apple trying to prevent the FBI from creating a backdoor into their phone encryption service (Apple, 2016). When the FBI could not convince Apple to do it, they got a German firm to do it for them. It didn't seem to matter what the legal terrain was, and it also didn't seem to matter what the technological hurdles were. As Gürses *et al* point out, searching for technological solutions to what is essentially a political problem is not going to ensure the democratic freedoms that the Fourth Estate has traditionally protected (Gürses et al., 2016). Nonetheless, having some skills in creating some barriers and protections around sources seems like the bare minimum a journalist should be able to provide. Many media organisations now have secure servers (*The Guardian* and *The New York Times* for instance) that can be found from their news sites, with instructions on how to download and use encryption tools such as Tor web browser technology.

But literacy with encryption doesn't overcome some of the problems of mainstream media organisations and their willingness to act upon information leaked to them. The rise of citizen journalism, WikiLeaks and other leak sites, and various Anonymous groups has introduced a new set of possibilities in the pursuit of accountability and transparency in a democratic society. It has been interesting to watch the trajectory of WikiLeaks as it finds a way to effectively carry out its mission of creating transparency in both government and corporate practices. As has been analysed in numerous academic articles (see for instance (Benkler, 2011; Goggin, 2013; Lidberg, 2013; Heemsbergen, 2015; de Zwart, 2013) WikiLeaks has enacted a variety of versions of 'radical transparency' which have involved the mainstream media in different kinds of relationships to the leaked materials.

[1] The manual "Information Security for Journalists" is available at: http://tcij.org/node/1016

The mainstream media in its turn has developed a range of different attitudes towards sites such as WikiLeaks. While making good use of the materials leaked through this site, there has also been a tendency to either dismiss WikiLeaks as a site of journalism, or to outright denigrate it as an irresponsible or reckless site that endangers society through its leaks. This has included, as Benkler (2011) points out, a lot of misreporting and misrepresenting of what has actually been released by WikiLeaks. The Cablegate releases for instance were often reported as a reckless release of thousands of documents, whereas in fact only several hundred carefully redacted cables that were perceived to be in the public interest were initially released. Subsequent release of the bulk of the cables was a result of press actions. There appear to be a number of dynamics in play here. One is the mainstream journalists perhaps attempting to guard the territorial boundaries of their profession. Another is the desire of the mainstream press to distance itself from prosecutable offences by letting sites like WikiLeaks take the fall.

WikiLeaks in its turn has clearly been working out the most effective ways to work in concert with mainstream media. Data dumps in themselves do not provide what it takes to get stories out – the distribution network and attention that mainstream outlets have is still a resource needed. But it is clear from the actions of Snowden, that some media organisations are seen to be more responsible and willing to act as government or corporate watchdog than others. Thus Snowden chose Greenwald and the *Guardian* as well as the *Washington Post*, but not the *New York Times*, which has been seen (along with the *Post* at times it has to be said) to be complicit with government and corporations more than as watchdog (de Zwart, 2013; Benkler, 2011, Harding, 2014, Greenwald, 2014). Further, journalists still play a vital role in the interpretation, analysis and organization of such data.

These new non-state, non-institutional actors can be seen as a catalyst for a media that may have grown complacent (Heemsbergen 2015). WikiLeaks is not the only player in this space of course. There have been other sites, such as Anonleaks, which more aggressively pursued transparency through hacking and was associated with the hacking groups of Anonymous. Rather than waiting for leaks to come to them, they took a more proactive stance to transparency, but as Heemsbergen points out, their actions didn't necessarily align with democratic values. Nikitina (2012) points to hackers as complicated figures who are occasionally aligned with the goals of democratic transparency and often not. In analyzing their role in the current context she characterizes them as full of contradictions and ambiguous. Although some may act in the interests of freedom of expression (for instance), most seem to not conform to expected norms and conventions or to have well thought through politics that inform their actions. However we would be wise not to dismiss the hackers. She suggests that in other times and in other cultures the figure of the trickster has worked as a transitional agent – one that is disruptive and creates uncomfortable yet revealing insights into a culture in transition (Nikitina, 2012). As Coleman's work has illuminated, hackers are variously motivated, only some working within a political framework of understanding (Coleman, 2014) and yet they may be a crucial part of the media ecology as the networked affordances are picked up and used by all stakeholders in the system. As governments and corporations explore the possibilities of data collection and surveillance offered by the new systems, and as mainstream media become ever more enmeshed in commercial and competitive goals, the leaks sites and the actions of hackers are playing unstable yet crucial roles in the scrutiny of those in power. They could be seen to be the actions of citizens on their own behalf in the face of the failing mechanisms of the press.

It is important to monitor the shifting pressure points created by government regulation: as national security concerns prompt tighter regulation of reporting of security activities and increased demands for access to metadata, government transparency and accountability appears to diminish. At the

same time recent work on whistleblowing has highlighted the importance of the insider in highlighting corporate, institutional or governmental wrongdoing (Lewis et al., 2014). This has led to enactment of enhanced whistleblower protection, provided that the whistleblower adheres to strict conditions. There are clear tensions here in terms of the values these pieces of legislation reflect. Meanwhile mainstream media is competing for ever diminishing public attention and dollars, and must be seen to be providing a value-added service. Some consideration needs to be given to the value of journalistic scrutiny in a democratic society to ensure that protections aimed at national security do not end up destroying the safety valve of a healthy and independent free press.

References

Andrejevic M. (2014) Wikileaks, surveillance, and transparency. *International Journal of Communication* 8: 2619-2630.

Apple. (2016) A message to our customers. (accessed 16 February 2016),http://www.apple.com/customer-letter/.

Benkler Y. (2011) A free irresponsible press: wikileaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review* 46: 311-397.

Berkman Center for Internet and Society T. (2016) Don't Panic. Making progress on the "Going Dark" debate. Cambridge MA: Harvard University.

Cole D, Hayden M and Garrett M. (2014) The Price of Privacy: Re-Evaluating the NSA, A Debate. *Johns Hopkins Symposium.* YouTube: Johns Hopkins University.

Coleman G. (2014) *Hacker, Hoaxer, Whistleblower, Spy. The many faces of Anonymous,* London, New York: Verso.

Coulthart R. (2015) Metadata access is putting whistleblowers, journalists and democracy at risk. *Sydney Morning Herald.* Sydney: Fairfax.

Day A and Molnar A. (2015) Data retention plan amended for journalists, but is it enough? *The Conversation*. (accessed 20 March 2015),https://theconversation.com/data-retention-plan-amended-for-journalists-but-is-it-enough-38896.

de Zwart M. (2013) Whistleblowers and the media. *Alternative Law Journal* 38: 250-254.

Doherty B. (2016) Offshore detention whistleblower loses job after condemning 'atrocity' of camps. *The Guardian Australia*. (accessed 21 June 2016),https://www.theguardian.com/australia-news/2016/jun/21/offshore-detention-whistleblower-loses-job-after-condemning-atrocity-of-camps.

Fernandez J and Pearson M. (2015) Shield laws in Australia. Legal and ethical implications for journalists and their confidential sources. *Pacific Journalism Review* 21: 61-78.

Ganesh MI and Hankey S. (2015) From information activism to the politics of data. *Fibreculture* 26: NP.

Given, J. (2007) Cross-Media Ownership Laws: Refinement or Rejection (Forum: Broadcasting and Media Laws) *UNSW Law Journal* (30)1:258-269

Goggin G. (2013) Democratic affordances: politics, media, and digital technology after WikiLeaks. *Ethical Space. International journal of communication ethics* 13: n.p.

Greenwald G. (2016) New Email Leak Reveals Clinton Campaign's Cozy Press Relationship. *The Intercept*. (accessed 11/01/2017),https://theintercept.com/2016/10/09/exclusive-new-email-leak-reveals-clinton-campaigns-cozy-press-relationship/.

Greenwald, Glenn (2014). *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* London, Hamish Hamilton.

Grubb B. (2014) Me and my metadata: How I beat Telstra after my 22-month legal battle. *Sydney Morning Herald*. (accessed 14 May 2014),http://www.smh.com.au/digital-life/digital-life-

news/me-and-my-metadata-how-i-beat-telstra-after-my-22month-legal-battle-20150504-1mz91c.html.

Grubb B. (2015) Minister for Encryption: metadata avoidance app Wickr shoots to top of charts after Malcolm Turnbull revealed as a fan *Sydney Morning Herald*. http://www.smh.com.au/digital-life/consumer-security/minister-for-encryption-metadata-avoidance-app-wickr-shoots-to-top-of-charts-after-malcolm-turnbull-revealed-as-a-fan-20150303-13tgxy.html.

Gürses S, Kundnani A and Van Hoboken J. (2016) Crypto and empire: the contradictions of counter-surveillance advocacy. *Media Culture and Society* 38: 576-590.

Gyles R. (2015) Report on the impact on journalists of section 35P of the ASIO Act. Independent National Security Legislation Monitor

Harding, Luke (2014). *The Snowden Files: The Inside Story of the World's Most Wanted Man* London, Guardian Books.

Heemsbergen L. (2015) Designing hues of transparency and democracy after WikiLeaks: vigilance to vigilantes and back again. *New Media & Society* 17: 1340-1357.

Holmes J. (2015) Data retention laws mean whistleblowers will become rarer and rarer *Sydney Morning Herald.* Sydney: FAirfax.

Keane B. (2013) Spy versus spy, gatekeeper versus gatekeeper. *Crikey.* Australia: Private Media Partners.

Lewis D, Brown A and Moberly R. (2014) Whistleblowing, its importance and the state of the research. In: Brown A, Lewis D, Moberly R, et al. (eds) *International Handbook on Whistleblowing Research.* Cheltenham, UK: Edward Elgar.

Lidberg J. (2013) From freedom to right - where will freedom of information go in the age of WikiLeaks. *Australian Journalism Review* 35: 73-85.

McNamara L. (2009) Counter-terrorism laws: how they affect media freedom and news reporting. *Westminster Papers in Communication and Culture* 6: 27-44.

MEAA. (2016) Criminalising the truth, suppressing the right to know. A report into the state of press freedom in Australia in 2016.

Murphy P. (2016) Journalists still face jail under Asio Act changes. *MEAA Media Release.*

Nikitina S. (2012) Hackers as Tricksters of the digital age: creativity in hacker culture. *Journal of Popular Culture* 45: 133-152.

Oakes L. (2016) "Media got complacent" *MEAA report Criminalising the Truth. Supressing the right to know. A report into the state of press freedom in Australia in 2016.* MEAA, 4-10.

Orner, Eva (2016). *Chasing Asylum*.

Pearson M. (2015) How surveillance is wrecking journalist-source confidentiality *The Conversation*. (accessed 22 June 2015),https://theconversation.com/how-surveillance-is-wrecking-journalist-source-confidentiality-43228.

Pusey, M. andMcCutcheon, M (2011) From the media moguls to the money men? Media concentration in Australia *Media International Australia incorporating Culture and Policy* 140: 22-34.

Rickertson M. (2013) Speaking truth to media power. *Australian Journalism Review* 35: 149-156.

Scahill, Jeremy and The Staff of *The Intercept* (2016). *The Assassination Complex: Inside the US Government's Secret Drone Warfare Programme* London, Serpent's Tale.

Thielman S. (2016) Facebook fires trending team, and algorithm without humans goes crazy. *The Guardian* (accessed 2 September 2016),https://www.theguardian.com/technology/2016/aug/29/facebook-fires-trending-topics-team-algorithm.

Turnbull M. (2012) Free at last! Or freedom lost? Liberty in the digital age http://www.malcolmturnbull.com.au/media/free-at-last-or-freedom-lost-liberty-in-the-digital-age-2012-alfred-deakin.

Vaughn, R. (2012) *The Successes and Failures of Whistleblower Laws* Cheltenham UK, Edward Elgar