Reuters Institute Fellowship Paper

University of Oxford

Bulk Collection: Broken Democracy?

Journalism and post-Snowden legislation

Comparative study: Australia and the United Kingdom

By Lisa Main

Trinity term 2016

Sponsor: ABC

Executive Summary

This paper aims to contribute to the debate over the impact of state surveillance on journalism. The mandatory bulk collection of data by governments presents liberal democracies with a dilemma. Can western governments maintain their commitment to a free press, something that distinguishes them from less savoury democratic regimes, whilst simultaneously compromising a fundamental principle of the journalism trade?

Bulk data collection means communication between a journalist and their source is recorded and can be accessed by the state – indeed, by the very authorities on which reporters are charged with maintaining an informal check of power. The temptation of governments to uncover the source of a damaging story is well known and documented. If sources or whistleblowers know they can be easily identified they are less likely to come forward, resulting in what's often referred to as the chilling effect.

Focusing on the post-Snowden era, this paper examines legislation governing the mandatory retention of data. It compares bulk data collection schemes in two liberal democracies; Australia and the United Kingdom. Both are parliamentary democracies and both are members of the Five Eyes intelligence sharing group.

Legal analysis was discussed with a wide variety of stakeholders, including a former British intelligence chief, the Australian Federal Police, constitutional experts, news editors as well as those responsible for oversight of data retention.

Despite similar government structures in the UK and Australia, the paper found that legislation in the respective countries took a divergent path. Journalists in the UK appear to have lost protections previously enjoyed whilst Australian journalists gained some safeguard provisions, albeit from a very low base.

In the United Kingdom the legal right of a journalist to protect the confidentiality of a source is established in law. A series of cases in the European Court of Human Rights set important precedents that informed the recent debate over the new Investigatory Powers Bill (IPB).

By contrast, the debate in Australia was engulfed in a climate of fear, partly encouraged by politicians as a response to the rise of terrorism. Unlike the UK, which is a signatory to the European Convention on Human Rights, Australia does not have a Bill of Rights. This unique constitutional setting left Australian journalists without similar legal precedents in relation to source confidentiality.

The legal provisions in bulk data collection schemes designed to protect a journalist's source and that of a free press more generally, known as safeguards and oversight, need to be strengthened in both countries.

Lisa Main 2016

This paper also found a challenging new set of legal circumstances for Australian journalists whereby not only can their sources be easily identified, but they are also subject to low threshold disclosure laws that carry criminal liability. This situation compounds the chilling effect and should be comprehensively reexamined by the parliament.

It should also be noted that this paper was written in the midst of change. The UK's Investigatory Powers Bill (IPB) was moving though parliament and at the time of publishing, the draft bill was being debated in the House of Lords. Thus details in this paper may not reflect the final form of the bill once it formally ascends into law.

Also during this time Britain voted to leave the European Union, David Cameron resigned as Britain's Prime Minister and was replaced by the former Home Secretary Theresa May.

If, as part of Brexit negotiations the UK withdraws as a signatory to The European Convention of Human Rights, journalists in the UK may no longer be afforded the legal protection to protect the identity of their source.

These conditions create an ominous harbinger for the core question confronted in this paper; can journalism and the surveillance state co-exist?

Acknowledgements

I'm enormously grateful to my employer, the Australian Broadcasting Corporation (ABC) for supporting me throughout this fellowship. I'd also like to thank my supervisor Chris Westcott for his patient ear, good humour and generous advice, James Painter for his tireless leadership, and David Levy for steering the impressive Reuters Institute ship. To my fellow fellows who inspired me everyday, I'll miss our talks, the tough questions, the after-class beers, laughs and tears. Lastly, my husband Hayden for proof-reading this paper, encouraging me throughout it, and allowing me to win on those sublime Oxford lawn tennis courts.

Table of Contents

BULK COLLECTION: BROKEN DEMOCRACY?

Introduction

In 2013, Edward Snowden's revelations of bulk data collection redefined the debate between the scope of state surveillance and the oversight of it. Over a period of eighteen months the Snowden reports gradually exposed the fragile legal basis upon which governments were relying to access the metadata records of their citizens.

The sequence of Snowden stories highlighted a fundamental question for liberal democracies, a question that turns on trust. How do governments maintain our hard fought-for liberal democratic freedoms whilst maintaining the capacity to retain the metadata of every citizen?

Surveillance is a deeply emotive issue.

One doesn't have to look far beyond liberal democratic borders to witness the manner in which omnipresent state surveillance is used as a devastating tool for censorship and repression, the essential weapon of tyrants.

The difference in liberal democracies is that 'lawful' surveillance is subjected to legal safeguards and independent oversight. The state and its security apparatus are bound by the rule-of-law.

Philip Bobbitt, a military strategist and constitutional academic who has served in both Republican and Democratic administrations in the U.S describes the dilemma as;

> *"The most difficult intelligence challenge of all… how to develop rules that will effectively empower the secret state that protects us without compromising our commitment to the rule of law".*[1].

[1] Bobbitt P, 2008, *Terror and Consent: the wars of the 21st Century*, Alfred A. Knopf, a division if Random House, New York

For journalists the dilemma is particularly acute. For them, a free press is dependent on respect for private communications and the fundamental and long-held principle that a journalist has a right to protect the identity of their source.

Metadata records can expose the identity of a journalist's source with astonishing ease.
As a result, societies that live with data retention enabled by both the corporate sector and the state, face a new paradigm. It's a paradigm in which journalists can no longer offer assurances of confidentiality to their sources.

That shift in social contract is compounded when sources are subject to low threshold anti-disclosure laws. If a source faces up to two years in prison for disclosing "any" information, as they do in Australia, and data retention enables the state to identify them with remarkable ease, then it's difficult to see how communications between journalists and their sources won't be affected.

But more critically, it is worthwhile examining if this new paradigm of data retention coupled with anti-disclosure legislation is congruent with the standards of a liberal democracy.

This paper examines one element of state surveillance, mandatory data retention, and compares the legal frameworks in two liberal democracies, Australia and the United Kingdom.

Chapter One examines Britain's post-Snowden data retention legislation and Chapter Two contrasts that experience with the introduction of similar legislation in Australia.

The paper compares the political framing of each country's data retention debate. How did each government engage the question of how they would manage these powers within rule-of-law principles?

Secondly, the respective datasets are examined. Thirdly, the paper considers the safeguard mechanisms and oversight of the bulk data retention schemes. And finally, a critique of the respective anti-disclosure legislation will discuss the impacts of data retention on leakers and whistleblowers.

Alongside a comparative analysis of legislation, this paper includes a discussion with a former GCHQ Chief, newspaper editors, lawmakers and journalists to examine the central question of whether data retention schemes and journalism can coexist within *liberal* democratic societies.

Literature review

When introducing data retention legislation, Attorneys-General from both Australia and the UK espoused their commitment to liberal democratic, rule-of-law principles.

Given the lack of a precise definition of democracy and its use as a broad defence by legislators when introducing data retention, this paper will first establish some definitional boundaries for a liberal democracy.

In 1946 George Orwell pointed out the lack of a clear definition of democracy and mused over why that might be the case.

> *"It is almost universally felt that when we call a country democratic we are praising it: consequently the defenders of every kind of regime claim that it is a democracy, and fear that they might have to stop using that word if it were tied down to any one meaning"*[2].

In recent decades, academics have begun to place some definitional specifics around the nature of democracies. In the late 1990s, Fareed Zakaria coined the term "illiberal democracy", identifying a political regime that holds elections but routinely violates civil rights. Zakaria noted that democracy had often been conflated with liberalism, mostly because western democracies since the end of World War Two have embodied both liberalism - the idea that an individual's human rights are protected and codified in law - and democracy, a system of elected government voted by the people.[3]

[2] Orwell G 1956, Politics of the English Language, in his *Collections of Essays,* New York, Harcourt Brace Jovanovich p. 156

[3] Zakaria F, 1997 *The Rise of Illiberal Democracy* Foreign Affairs, November/December issue

BULK COLLECTION: BROKEN DEMOCRACY?

In a series of essays on democracy and surveillance Kevin Haggerty and Minas Samatas argue a vital aspect of democracy is accountability. Citizens have the right to vote for or against elected representatives.[4]

> *"Accountability therefore implies that citizens need access to a range of information about the actions of their representatives and a free press to assess the behaviour of their government."*[5]

More recently, U.S academics Dani Rodrik and Sharun Mukand built on Zakaria's earlier work and unpacked the concepts of "democracy" and "liberalism".[6] Their distinctions are particularly relevant and serve as a definitional framework for this paper. According to the authors, liberal democracies protect three sets of rights; property rights, political rights and civil rights.

Property rights protect citizens against expropriation by the state; political rights empower the majority; and civil rights protect the minority. According to Mukand and Rodrik, liberal democracies demand all three.

Democracies that only adhere to the first two are defined as 'electoral' democracies and include OECD members Israel, Hungary and Mexico among others[7]. Mukand and Rodrik point out a common characteristic of 'electoral democracies' is *"censorship or self-censorship in the media"*[8].

---

[4] Haggerty K.

D, Samatas, 2010, *Democracy and Surveillance,* Routledge, United Kingdom, p. 21

[5] Haggerty K.D, Samatas, 2010, *Democracy and Surveillance,* Routledge p. 2

[6] Mukand S, Rodrik D, 2015 The Political Economy of Liberal Democracy, Working Paper available at Working Paper 21540 [online] http://www.nber.org/papers/w21540

[7] ibid p. 3

[8] ibid p. 3

BULK COLLECTION: BROKEN DEMOCRACY?

In 2016, Freedom House reported press freedom to be at its lowest levels in 12 years. Only 13% of the world's population enjoyed a free press[9]. In worldwide freedom of the press rankings Australia was placed 23rd, just above the UK in 25th position. Whilst both countries are considered "free", Australia comes under criticism for its 2015 data retention legislation and anti disclosure laws.

The UK is criticized for its proposed Investigatory Powers Bill (IPB). Both issues will be discussed further in the paper.

In her 2010 book "The Silent State", UK based journalist and academic Heather Brooke points to a "double standard", describing the disconnect between the state's increasing lack of openness whilst it simultaneously imposes intrusive surveillance on its citizens.

> *"Surveillance is not about keeping us safe, it's about power; who has it, and who doesn't. Currently the state has it and the citizens don't."*[10]

Brooke concludes that Britain has already fallen short of a democracy because surveillance laws "run foul" of privacy and human rights law. According to Brooke, the social contract is broken.

Canadian Law professor and author Lisa Austin argues a serious rule-of-law problem exists post-Snowden. Austin notes that whilst legal pathways exist for state surveillance, the absence of oversight and accountability demanded by the rule-of-law has created a situation she describes as "lawful illegality[11]."

---

[9] Freedom House 2016, *Press Freedom Index*, [online] https://freedomhouse.org/report/freedom-press/freedom-press-2016

[10] Brooke H, The Silent State: Secrets, Surveillance and the Myth of British Democracy

[11] Austin L, (2015) Lawful Illegality: What Snowden has Taught us about the legal infrastructure of the Surveillance State, In: (eds.) Michael Geist, Law Privacy and Surveillance in Canada in the post-Snowden Era, Canada, University of Ottawa Press, Ch. 4, p.103-125.

BULK COLLECTION: BROKEN DEMOCRACY?

Lawful illegality is more visible post Snowden but it's not entirely new.

In 1992 Criminologist Robert Reiner coined the term 'blue-letter law', described as a discretionary legal tool box for the purpose of policing[12]. Reiner differentiated blue-letter law from the traditional black-letter law, or rule-of-law, where the doctrine insists that the law binds governments and their officials, just as much as it does everyone else, to a set of rules.

Reiner sates that "the majority of police actions, such as the power to apprehend, question and use force would be serious criminal offences if they were not done under the cover of legality". Thus, police 'rule with law'.[13]

Until recently, these capabilities have been used and directed only at suspected criminals. It can be argued that data retention subjects every citizen to a form of blue-letter law.

'Counter-law' is a concept identified by Criminologist Richard Ericson and described as "the technique of using law against law".[14] Ericson argued that heightened attention on security legislation resulting, in part, from the threat of terrorism saw politicians respond to potential threats of harm with legal measures that suspend, or clash with the conventional 'rule-of-law' order. Ericson argues periods of heightened security risks have been normalised.

> *"The declaration of the state of exception has been replaced by an unprecedented generalisation of the paradigm of security as the normal technique of government."*[15]

[12] Reiner, R. 2000, *The Politics of the Police*, Oxford University Press, New York 3rd ED p. 87

[13] Ibid, p.88

[14] Ericson, 2007, *Crime in an Insecure World*, United Kingdom Polity Press Cambridge p. 24-31

[15] Ibid. p26

Ericson's term 'counter-law' describes how legal measures designed to protect national security nullify the effects of other legal instruments. His work discusses the importance of understanding how national security measures are proposed and justified.

Ericson's 'counter-law' conundrum becomes relevant to journalists in the post-Snowden environment. Journalists argue that it's what the law allows that is the problem, the dilemma of lawful illegality.

1. United Kingdom

Post-Snowden Legislation

The post-Snowden debate over bulk data retention was markedly different in Australia and the UK. Australia's debate was characterized by an urgent need to pass anti-terrorism legislation in response to fear of attacks on home soil.

In Britain, the debate was by and large, a response to Snowden.

The initial conundrum for the Guardian newspaper was how to publish the first Snowden story without facing a legal injunction from the British government. The revelations would likely be viewed as damaging to national security and thus the state could apply an injunction to halt publishing. [16]

Guardian Editor at the time of Snowden, Alan Rusbridger bypassed the informal DA-Notice system where editors can check if a story carries a risk to national security.

[16] BBC 2013, David Cameron criticises the Guardian for publishing Snowden data, October 16, 2013 *BBC* [online] http://www.bbc.co.uk/news/uk-politics-24555955

> *"We didn't use it for the very first story because I didn't trust it really, I found it hard to understand how if you rang up a retired Wing Commander or Admiral and said 'look we are about to publish this stuff about GCHQ from Edward Snowden', how the Chinese walls within Whitehall could possibly work".*

(Alan Rusbridger in an interview with the author of this paper May 2016)

The second test came when the government requested the Guardian voluntarily destroy the Snowden files. Rusbridger said if the Guardian did not comply, the government would have sought a legal injunction to force the Guardian to hand over the documents.

The Guardian took the decision to destroy the Snowden documents but continued to publish from the United States where journalists are protected by the first amendment.

> *"When we were working with Wikileaks and on Snowden with the New York Times and Pro Publica, to begin with I was horrified when they said we were going to go to the government a week in advance, because that would be a disaster in the UK but they had a mature understanding in which they could have that conversation and sometimes that does enable the government to use forms of emotional blackmail or whatever but they can't use the law and that's the difference"*

(Alan Rusbridger in an interview with the author of this paper May 2016)

According to Anthony Glees, Director of the Centre for Security and Intelligence Studies at the University of Buckingham, the government took an early decision not to publically inflame the surveillance debate.

> *"The moment the government discovered the disclosures that Edward Snowden was about to make it took a decision not to fight Snowden. It [the government] was going to appease its way out of the problem."*

(Anthony Glees in an interview with the author of this paper June 2016)

For its subsequent Snowden stories, the Guardian made use of the UK's DA-Notice system. As the revelations continued public debate broadened and the legal ambiguity in which data retention was governed began to be prosecuted in the courts.

As a result of the revelations, in February 2015, the Prime Minister's own intelligence watchdog, the Investigatory Powers Tribunal (IPT) found GCHQ had breached human rights conventions in relation to the UK's access to the NSA's bulk data collection program.[17]

The IPT found that GCHQ was non-compliant with Article 8 and Article 10 of the European Convention of Human Rights. Article 8 refers to the Right to Privacy and Article 10 refers to Freedom of Expression. The IPT ruled that GCHQ acted unlawfully because it had not disclosed how data sharing arrangements were authorised nor did the agency identify the safeguards used in the secret program.[18]

All parties claimed victory after the ruling. The government and the intelligence agencies claimed it affirmed the legality of their bulk data collections. Their view was that the agencies simply needed to provide more detail about the safeguards to the public. But privacy advocates claimed the ruling confirmed the existence of illegal mass surveillance programs by GCHQ.

[17] BBC 2015, GCHQ censured over sharing of internet surveillance data with US, *BBC* February 6, 2015 [online] http://www.bbc.co.uk/news/uk-31164451

[18] ibid

The debate remains unsettled. The ruling is a clear example of how Reiner's blue-letter law has led to a situation of 'lawful illegality' where legal pathways for surveillance exist but without the oversight demanded by the rule-of-law.[19]

Another Snowden issue tested in the courts was the questioning of David Miranda.

David Miranda, the partner of Guardian journalist Glenn Greenwald, was detained and questioned by the UK's Metropolitan police when leaving Heathrow Airport. Miranda was thought to be carrying some Snowden files and was questioned for nine hours under Schedule 7 of the UK's Terrorism Act, generally known as 'the stop power'.

Schedule 7 allows authorities to stop and question travelers to establish if they *appear* to be a terrorism threat. In the legislation, 'terrorism' is broadly defined and David Miranda was not entitled to legal representation throughout his nine hours of questioning. [20]

Earlier this year, the UK Court of Appeals found that whilst the Metropolitan police "lawfully" detained David Miranda, the use of 'the stop power' when applied to a journalist's material was incompatible with Article 10 of the European Convention on Human Rights - Freedom of Expression.[21]

[19] Austin L, 2015, *Law Privacy and Surveillance in Canada in the Post-Snowden Era*, University of Ottawa Press, Canada

[20] BBC 2013, David Miranda Detention: MP asks police for explanation, *BBC,* August 19, 2013[online] http://www.bbc.co.uk/news/world-latin-america-23750289

[21] *David Miranda vs. Home Office Met Police UK Court of Appeals,* January 19, 2016 https://www.judiciary.gov.uk/wp-content/uploads/2016/01/miranda-v-home-sec-judgment.pdf

> *"If journalists and their sources can have no expectation of confidentiality, they may decide against providing information on sensitive matters of public interest.*[22]

The European Court of Justice (ECJ) delivered a more significant setback to the UK's data retention scheme. On April 8, 2014 in the joint cases of Digital Rights Ireland and Kärntner Landesregierung the ECJ ruled the UK's Data Retention Directive 2006 to be invalid. The ECJ listed five failings of the data retention directive, among them was the lack of safeguards and oversight[23].

The ruling left the UK government exposed. The current Investigatory Powers Bill (IPB) is a response to both the ECJ ruling and Snowden[24] . The expansive surveillance bill is touted as an effort to ensure the state's surveillance powers are on a firm legal footing but the problem of lawful illegality persists. To ensure rule-of-law principles are not eroded the state must satisfy itself that the IPB's safeguards and oversight are sufficiently independent and robust enough to withstand a challenge in the ECJ.

Anthony Glees believes intelligence and law enforcement agencies should have access to the powers outlined in the IPB but warns that great care must be taken in drafting the legislation.

> *"A government can declare something to be lawful that shouldn't be lawful. Look at the trouble George W. Bush's White House got into getting lawyers to say waterboarding and other forms of physical abuse weren't torture, they set a [legal] bar*

---

[22] 2016, Terrorism act incompatible with human rights, court rules on Miranda Case, Owen Bowcott, January 19, 2016 , https://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case

[23] Heitzer S, Kuhling J, 2015, Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24 in the UK and elsewhere, *European Law Review*, case Comment p.2

[24] Draft Investigatory Powers Bill (IPB), 2015 UK Parliament [online] http://services.parliament.uk/bills/2015-16/investigatorypowers.html

> *then they themselves decided they didn't cross that bar but world public opinion decided that they did, it was an abuse of the law."*

(Anthony Glees in an interview with the author of this paper, June 2016)

The purpose of the IPB is to replace existing powers with a single statute that, according to the UK's Attorney-General, *"strikes a balance between democratic accountability and independent judicial scrutiny of the exercise of the most intrusive powers*".[25]

The following chapters explore this question of balance first by identifying what data the UK government is proposing to collect and then examining the safeguards and oversight provisions.

[25] 2015, The Bar Blog, The Attorney General on the Investigatory Powers Bill, December 10, 2015 [online] http://www.barcouncil.org.uk/media-centre/bar-blog/contributing-writers/2015/december/attorney-general-on-the-investigatory-powers-bill/

The Dataset

The UK's Investigatory Powers Bill (IPB) legislates for a broad range of intrusive powers including phone interception and computer hacking. Data retention is only one component of the bill and the only component examined in this paper as it offers a direct comparison with similar legislation in Australia.

Whilst the government insists all of the powers outlined in the IPB bill are already available in other legislation, data retention is the exception, a point acknowledged in a foreword note on the draft legislation.

> *"The draft Bill only proposes to enhance powers in one area—that of communications data retention—and then only because a strong operational case has been made."*[26]
>
> (Former, UK Home Secretary, and current British Prime Minister Theresa May.)

Datasets determine what data governments request telecommunications companies to retain as part of their bulk collection regimes. The language used to identify datasets is legalistic, broad and technology-agnostic. This is so the legislation does not have to be updated each time a new technology comes online.

For example, the internet of things, machine to machine communication and cloud computing apps all represent a quantum leap in technological capability and redefine how humans interact with technology.

[26] Draft Investigatory Powers Bill, Cm 9152, November 2015, p1 [online] https://www.gov.uk/government/publications/draft-investigatory-powers-bill

To keep pace with this change, datasets need to be flexible. Yet at the same time, specific enough so the legislation can also protect a citizen's privacy and communications between a journalist and a source.

The UK's IPB dataset is split into two categories;

1. Communications Data (CD) - The Home Office defines CD as the 'who', 'when', 'where' and 'how' of a communication, often referred to as its 'metadata'. It also includes partial internet connection records - any information up to the first forward slash of a web address. For example, bbc.co.uk/ or facebook.com/

2. Content - includes the voice recording of your Skype conversation or the body of an email as well as internet connection records (ICR's) e.g. bbc.co.uk/ChilcotReport

To access 'content' an authorised public servant would require a warrant. But a warrant is not required to access 'communications data' unless the person is a journalist or the intent is to uncover the identity or confirm journalistic sources[27].

Former GCHQ Chief and Visiting Professor at the Department of War Studies, King's College, London Sir David Omand served as an expert witness to the parliamentary committee overseeing the UK's dataset[28].

> *"Communications Data in UK law is not the same as 'metadata' [where] the most sensitive parts of which count as content and would need a warrant."*

[27] Investigatory Powers Bill 2016, HL Bill 40, Part 3, Authorisations for obtaining communications data, section 73 [online] http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

[28] 2016 House of Comms Third report, Science and Technology Committee [online] http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf

(Sir David Omand in an interview with the author of this paper June 2016)

Joss Wright from the Oxford Internet Institute joined Sir David Omand as an expert witness examining the UK's dataset. Wright sees the distinction of Communications Data as 'less sensitive' than content as a false dichotomy. He gives the example of your Netflix account. According to Wright, the film (the content), meaning what the actor is doing at any one moment on screen, is less sensitive than the information about what you watch, when you watch, how often you watch it and with whom - the Communications Data.

> *"Metadata and content data are being used as a proxy for what is non-sensitive and what is sensitive and if that's the clause that we want to see, that some data is more sensitive, then we should make that distinction. We shouldn't be wrapping it up in this pseudo definition that sweeps all of the complexity under the carpet and that's what's happening in this debate."*

(Joss Wright in an interview with the author of this paper June 2016)

Another issue highlighted by the National Union of Journalists (NUJ) is the ownership of the communications data. As the bill stands, internet or communication service providers (ISP's/CSP's) own the communications data. That includes the telephone numbers dialed by a journalist and those from which the journalist has received calls.

> *"There's no difference in our minds between the police getting hold of the traditional reporter's notebook, or getting their hands on our emails, metadata, or bugging our activities by remotely activating mobile phones. Journalistic materials and communications data should have equal status and protections in law and communications data should be defined as belonging to the journalist."*

(Michelle Stanistreet, General Secretary of the NUJ in an interview with the author of this paper July 2016)

Ownership of communications data becomes an issue for journalists who seek to protect the identity of their sources. If journalists don't own their communications data (information that would have sat in their notebooks a decade ago) how can they defend it in court?[29]

> *"We continue to hear from government that communications data belongs to the service provider but I doubt that is how most people, citizens or journalists, would view the ownership of their information. We continue to argue with politicians that a journalist must be notified in advance of accessing their communications data because if a journalist does not know that their data is being snooped on and their sources spied on, then the journalist cannot defend themselves or the long-held principle of the protection of sources. This principle goes to the heart of our campaigning work on the Investigatory Powers Bill."*

(Michelle Stanistreet, General Secretary of the NUJ in an interview with the author of this paper July 2016)

Alan Rusbridger sees the shift of ownership of digital communications data as "extraordinary". Rusbridger says conventions of privilege that were built up over the past 200 years, between doctors and patients, lawyers and clients, and journalists and their sources have been swept away.

> *"People have decided that it's ok to treat digital information differently from physical information… so all of these conventions that grew up over centuries are now not observed and police forces and intelligence agencies have just decided they are not going to respect them. I don't know how we allowed that to happen but it has happened."*

(Alan Rusbridger in an interview with the author of this paper May 2016)

[29] European Court of Human Rights [online] http://hudoc.echr.coe.int/eng?i%3D001-57974#{"itemid":["001-57974"]}

Safeguards

A 2015 report by the UK's Interception of Communications Commissioner (IOCCO) demonstrated how police shopped around for legislation that would enable them to access journalists' communications data without seeking a warrant.[30]

The IOCCO report found that police accessed the communications data of 82 journalists over a three-year period. The Commissioner concluded that police forces *"did not give due consideration to freedom of speech*".

In the UK, the Police and Criminal Evidence Act 1984 (PACE) is the legislation designed to enable law enforcement to access a journalist's communications data for the purposes of a criminal investigation. The legislation requires the police to apply to a judge when they seek to uncover the identity of a journalist's source. Under the legislation, journalists are notified and are entitled to contest the warrant in court.

Yet in 82 instances police bypassed PACE legislation. Instead the police used, or more accurately misused, another piece of legislation, the Regulation of Investigatory Powers Act (RIPA).

The IOCCO 2015 report found 19 police forces had made 608 applications using RIPA legislation instead of PACE[31]. The report found the application process designed by the UK's Home Office focused on privacy considerations but offered no guidance on how police might consider their obligations under Article 10 of the European Human Rights Convention, Freedom of Expression.

Two decades ago, in 1996, the landmark case, Goodwin v the United Kingdom ruled that identifying a journalist's source was a contravention of Article 10 (Freedom of Expression) *"unless justified by an*

[30] Interception of Communications Commissioner, *Inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources*, February 4, 2015

[31] Ibid.

overriding requirement in the public interest"[32]. Since then, the UK's National Union of Journalists (NUJ) has won numerous cases using this ruling as a precedent.

Following the IOCCO report, the UK parliament revised the code of practice for police governing access to a journalist's communications data. The revised codes stipulated that police must use PACE to seek access to a journalist's communications data, unless there was an immediate threat to life, in which case, the police could use RIPA and avoid seeking a warrant.

Under the PACE legislation, to issue a warrant a judge must be satisfied that a serious offence had been committed; that the communications data would be admissible evidence in court and that other methods of obtaining it have been tried or deemed unachievable. Most importantly, access to a journalist's communications data must be in the "overwhelming" public interest.[33]

Yet, just three months after the revised codes came into force the IOCCO found police had again used RIPA to seize call and text logs from the phones of journalists without judicial approval.

In response to the findings the IOCCO Commissioner, Sir Anthony May wrote to the UK's Prime Minister David Cameron expressing his deep concern about the "serious contraventions".[34]

Since then, all changes concerning PACE and RIPA have been deferred to the Investigatory Powers Bill (IPB) which at the time of writing, was being debated in the House of Lords.

---

[32] European Court of Human Rights, *Fact Sheet Protection of journalistic sources*, 2016, [online] http://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf

[33] UK House of Commons Briefing *Access to Journalists' Sources*, No. 07440, 31 December 2015 p. 5

[34] Interception of Communications Commissioner, *Half-yearly report*, HC 308, 16 July 2015, para 3.21 p. 10

In its current draft, the IPB does not maintain the same protections as PACE.

The IPB stipulates a judicial warrant, known as a 'double lock' measure because it requires both ministerial and judicial approval before access to a journalist's communications data is granted. Still many journalists see the 'double lock' as little more than a rubber stamp process where the judge only examines the process and not the 'public interest'.

The National Union of Journalists is seeking similar protections in the IPB that are offered under the PACE legislation.

> *"The NUJ has a strong track record of being able to defend sources using this legislative framework. We are not convinced that the current approach set out in the IPB, including a 'double lock' creates any significant protections for journalists."*

(Michelle Stanistreet, General Secretary of the NUJ in an interview with the author of this paper July 2016)

Even so, Alan Rusbridger says there will always be someone who is prepared to 'risk it all' like Edward Snowden, but he sees a looming situation where the free flow of information slows. Rusbridger refers to everyday information exchanges between a journalist and the plethora of civil servants who help journalists understand issues and thus report more accurately. Confidentiality is crucial to these relationships and enables journalists to fulfil their function as the informal check on power. Those communications could be with a health care worker, a school teacher or a treasury official and they are often unauthorized.

> *"The question needs to be put to government…do they recognise that the most valuable information journalists handle is unofficial information, and that is often to the public benefit. These would be good assertions to get on the record that the government accepts if not we're going back to the dark ages of information. That is an urgent question to establish because you can't really work out the practicalities of the law until you have that sorted out."*

(Alan Rusbridger in an interview with the author of this paper May 2016)

As the IPB moves though both houses of parliament, several amendments have been proposed to strengthen the safeguards and bring them into line with the PACE provisions, namely prior notification whereby a journalist is notified if a warrant has been sought on their metadata.

> *"It is all very well having judicial safeguards in place, but they will not work unless the judicial commissioner assessing the application has all the relevant information before applying his or her judgment and making an informed decision. After all, how can a judicial commissioner possibly know what they do not know? That is almost Kafkaesque."*

(Lord Black of Brentwood, House of Lords debate, June 27, 2016,)

When introducing the Investigatory Powers Bill into parliament, then Home Secretary Theresa May asserted the bill "*will provide some of the strongest protections and safeguards anywhere in the democratic world"*[35].

The veracity of Theresa May's remarks remains to be proven but she perhaps misses the point. The seminal question and overarching test of the legislation should be, is the bill compatible with the principles of a liberal democracy, because not all democracies protect civil rights. In fact, few do, and when they don't, censorship or self censorship of the media occurs.

[35] 2015, The UK government has revealed how it wants to spy on citizens, Sam Shead, Business Insider, November 4 , 2015 [online] http://uk.businessinsider.com/uk-government-draft-investigatory-powers-bill-how-it-wants-to-spy-on-citizens-2015-11

Oversight

> *"Britain suggests poor oversight because the ISC [the UK's Intelligence and Security Committee] missed all of the post 9/11 controversies, Iraq's weapons of Mass Destruction, extraordinary rendition and the July 2005 bombings, each time it took other inquiries to get to the truth."*

(Senior UK security journalist in an interview with the author for this paper June 2016)

In his report, A Question of Trust, David Anderson QC, the UK's independent reviewer of anti-terrorism legislation observed that the UK's intelligence agencies are coming to terms with the realisation that the secretive nature of their work requires institutional safeguards and direct public engagement[36].

When publishing the Snowden stories, then Guardian Editor Alan Rusbridger struggled to reconcile how a part-time oversight committee, "consisting mostly of retired parliamentarians" could offer "anything that looked like meaningful oversight". The lack of technical expertise and independence are commonly talked about as serious shortcomings of the UK's oversight bodies by interviewees for this paper.

> *"When I saw the [Snowden] documents it took hours and hours of work to understand what they meant because these [intelligence] documents are full of jargon and refer to everything by acronym….So [the part-time committee] has some sort of technological expert who is by your side and I asked a guy [on the committee] and he said 'oh yes we have someone who is very good, he's former GCHQ'. So their outsider technical expert was a retired insider."*

(Alan Rusbridger in an interview with the author of this paper July 2016)

[36] Anderson D, 2015, *A Question of Trust: Report on the Investigative Powers Bill Review* [online] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf p. 191

Yet oversight of data retention is considered vital for maintaining the integrity and public trust in the intelligence and government agencies which have access to bulk communications data. The public must be confident that access won't be abused.

In his 2010 book, Securing the State, Sir David Omand points out that human rights are a public good, as is security, and methods used must be in keeping with rule-of-law principles, for which oversight is key.

> *"The system of oversight depends crucially on the existence of trust in the integrity of the scrutineers and robustness and independence from government over the scrutiny."* [37]

Oversight of the UK's security and intelligence agencies is currently spread over a number of bodies and subject to varying statutes.[38] In an effort to build public trust, the Home Secretary claimed the IPB would build a *"world-leading oversight regime".* To achieve this end the UK is completely overhauling existing oversight structures.[39]

The IOCCO will no longer exist when the bill comes into force. The body will be replaced by the office of the Investigatory Powers Commissioner, to be supported by a number of Judicial Commissioners, thought to be six or seven. However, these commissioners will only be responsible for overseeing

[37] Omand D., 2010, *Securing the State,* C. Hurst & Co, London p.265

[38] 2015 Home Office Impact Assessment Oversight, Investigatory Powers Bill [online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473777/Impact_Assessment-Oversight.pdf

[39] 2015, Theresa May Investigatory Powers Bill Speech [online] November 4, 2015 [online] https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

applications that require warrants to communications data and content, thought to be roughly two percent of the data retention scheme.

The remaining 98 percent will be post-facto oversight carried out by specialist technical inspectors. The draft legislation stipulates that the UK Secretary of State will determine the budget for the specialist inspectors overseeing the vast majority of the data retention regime. This potentially creates a conflict of interest because the Secretary of State will allocate the budget for reviewing law enforcement agencies which answer to the Secretary of State[40].

To avoid this situation the IOCCO, David Anderson QC and the RUSI report all recommended an independent Oversight Commission be established which would include the Commissioners as well as the technical staff who will carry out the overwhelming majority of the work.[41] This issue is yet to be resolved.

In comparison with Australia's oversight structures, there is one notable difference; the deterrent of criminal liability for officials who abuse their access to communications data.

In the draft UK legislation, unlawful access by a public official to communications data is a criminal offence punishable by up to two years in prison.[42] Australia has no such deterrent. Further, if an Australian journalist discovers a warrant has been sought on their metadata and they then report that

[40] 2016, IOCCO Points to Consider on the IPB March 1, 2016 [online] http://www.iocco-uk.info/docs/Points%20to%20Consider%20on%20IP%20Bill%20and%20recommendations%20-%20updated%20post%201st%20March%20amended%20Bill.pdf

[41] Ibid

[42] Investigatory Powers Bill [online] http://www.parliament.uk/documents/commons-public-bill-office/2015-16/compared-bills/Investigatory-Powers-bill-160505.pdf

information, the journalist could be found liable under anti-disclosure clauses and face two years imprisonment[43].

Although considered efforts are being made in the UK to ensure oversight of surveillance is no longer latent the widespread perception among journalists remains. Journalists interviewed for this paper agreed that despite the proposed oversight provisions outlined in the IPB, the risk of abuse persists. One interviewee added that the journalists weren't alone in their concern.

> *"Because of events in recent years the perception in parliament is that the risk [of abuse] comes from police rather than intelligence services, whether that's actually the case, is another thing."*

(Senior UK security journalist in an interview with the author of this paper July 2016)

In this post-Snowden environment, Sir David Omand reflects on the imperfect nature of oversight and the role of the fourth estate.

> *"In an ideal world there would be sufficient transparency for Parliament to assess the public interest in legislating for and then overseeing intelligence matters. But I accept we are in an imperfect world hence my support for a free press - provided it thinks about the consequences of its actions in exposing matters considered secret by the authorities, takes advice before publication, and then makes its own decisions in its view of the national interest - not just their interest in a scoop, circulation or selling space on their media. Public interest in a story is not the same as a story being in the public interest."*

(Sir David Omand in an interview with the author of this paper June 2016)

---

[43] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Australia *182A Disclosure/use offences: journalist information warrants*

Communications Data and Disclosure Legislation

> *"You don't want a free-for-all with state secrets, some journalists publish carelessly with sensitive material. I'm not going to expose any active intelligence operation. I'll only do that if there are breaches of human rights"*[44]

(Stephen Grey, Reuters journalist and author of The New Spymasters in an interview with the author of this paper, June 2016)

Unlike Australia, the full extent of the UK's anti-disclosure laws has not been comprehensively mapped as it was by the Australian Law Reform Commission.

When Australia's Law Reform Commission studied the full suite of anti-disclosure laws in 2010, it found 506 secrecy provisions in 176 pieces of legislation[45].

This chapter does not attempt to undertake that enormous task for the UK, rather it deals with anti disclosure laws that carry criminal punishments for a source and/or a journalist.

Journalists working in the UK who were interviewed for this paper didn't fear prosecution under Britain's anti disclosure laws. Instead, it was unanimously felt that the source was more exposed. The problem for journalists reporting on intelligence, defence and national security issues was how to quantify the risk their sources were taking.

> *"There are so few cases that knowing where the lines are is very hard, there isn't a lot of precedent".*

---

[45] Australian Law Reform Commission Report Secrecy Provisions 2010, [online] http://www.alrc.gov.au/publications/3-overview-current-secrecy-laws/specific-statutory-secrecy-provisions

(Senior UK security journalist in an interview with the author of this paper, July 2016)

The UK's Official Secrets Act 1911 is the overarching legislation that criminalises unauthorised disclosures by intelligence and defence officials in the UK. Figures on the number of prosecutions under the Act have never been published but are thought to be fewer than one per year.[46] Prosecutions rarely involve the journalist, mostly the source.

The Act was introduced in response to fears over German spying and the decision to prosecute someone under the Act lies with the Attorney-General. [47]

The maximum punishment under the Official Secrets Act 1911 is fourteen years in prison, however consecutive sentences carrying lifetime prison sentences are possible.

Up until 1989, the Official Secrets Act retained a "catch-all" clause in section 2 where disclosing "any" official information without lawful authority was a criminal offence.

The "catch-all" clause was eventually repealed as it was found to be "unsatisfactory" by the 1972 Franks Report[48].

> *"Its scope is enormously wide. Any law which impinges on the freedom of information in a democracy should be much more tightly drawn.[49]*

[46] ibid p. 5

[47] 2015, House of Commons Report, The Official Secrets Act and Official Secrets, December 17, [online] http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7422 p. 2, 4

[48] Ibid p15

[49] Ibid p. 17

In Australia, an almost identical "catch-all" clause in Section 70 of the Crimes Act remains in place and is routinely used to trigger leak investigations. This law will be further discussed in the following chapters on Australia.

Despite the Franks report, it took the UK almost twenty years to repeal its "catch-all" disclosure laws. The 1989 Official Secrets Act tightens the "catch-all" phrase and applies to disclosures concerning security, intelligence, defence as well as international relations. To secure a successful prosecution the government must prove that the disclosures are damaging to the state. There is no public interest defence[50].

> *"There is legal, illegal [disclosures] but then there are those cases that will be prosecuted, it's all about how you can navigate the system."*

(Stephen Grey, Reuters journalist and author of The New Spymasters in an interview with the author of this paper, June 2016)

For some journalists the solution for dealing with high-risk unauthorised disclosures is using encryption and in some cases operating completely offline.

> *"You can never say to a source there is no risk, the problem now is that [data retention] makes it easier to identify sources. Most forms of encryption can trip you up, they create a false sense of security. The best tactic is to create noise, if you're constantly on the phone to masses of people, you create a lot of noise and it's more difficult for them [law enforcement and intelligence] to cut through".*

(Stephen Grey in an interview with the author of this paper, June 2016)

[50] Ibid. p. 17

BULK COLLECTION: BROKEN DEMOCRACY?

Bulk data regimes dissolve the idea that communications between a journalist and a source can be kept confidential. Access to communication data records increase the likelihood of prosecution should the government choose to pursue an unauthorised disclosure.
For journalists the long held principle that sources could talk to them without being identified by the government no longer holds, but there are broader implications.

> *"If you make it harder for someone to offer information then you are inhibiting the flow of information and that makes the press a weaker instrument and less able to hold power to account. You may not intend to do that but that's what's going to happen. That's why you have to get people who are passing these laws to state whether or not they believe in a free press. If they don't then they shouldn't be in power, but it would be interesting to pin them down on that."*[51]

(Alan Rusbridger in an interview with the author of this paper, May 2016)

1. Australia

Post Snowden Legislation

The post-Snowden data retention debate witnessed in the UK was not replicated in Australia. Instead, the political rhetoric that framed the introduction of Australia's bulk data retention scheme centred on the rise of Islamic State (ISIL).

In an address to Parliament on the 22nd September 2014, Prime Minister Tony Abbott, a former journalist himself, primed Australians for what was to come.

> *"Regrettably, for some time to come, Australians will have to endure more security than we are used to and more inconvenience than we would like. Regrettably, for some time to come, the delicate balance between freedom and security may have to shift."*[52]

But that 'delicate balance' was drawn from an unusual base. Australia is unique among liberal democracies in that it does not have a Bill of Rights. Despite ratifying the UN International Covenant on Civil and Political Rights, the treaty has never been adopted into Australian law.

In contrast, Britain is a signatory to the European Convention on Human Rights (ECHR) and any breach of the charter can be referred to the European courts, as happened in the Digital Rights Ireland case[53].

> *"So we have none of the protections that the European countries nor North American or New Zealand have to allow the courts to reach a view that would be consistent with Freedom of Speech…but the High Court has implied a right of political communication,*

[52] 2014, Australian Commonwealth, *Parliamentary Debates*, House of Representatives, No. 9957, 22 September 2014

[53] Heitzer S, Kuhling J, 2015, Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24 in the UK and elsewhere, *European Law Review*, case Comment p.2

> *implied because you cannot have a modern democracy without the right to communicate for political reasons".*

(Australian Human Rights Commission President, Professor Gillian Triggs in an interview with the author of this paper, May 2016)

In late 2014 Australia's Attorney-General, George Brandis QC set out his position on the data retention debate as he introduced a series of counter-terrorism laws. The Attorney-General assured the public that the new powers would not diminish Australia's commitment to the rule-of-law.

> *"As a lawyer, I have a bred-in-the-bone respect for due process and the rule-of-law. As a liberal, I have an instinctive reluctance to expanding the power of the state or diminishing the freedom of the individual."*[54]

Prior to Australia's parliamentary metadata retention debate, more than eighty Australian government agencies had, for decades, been routinely accessing metadata records of citizens and journalists.[55] No warrant was required.

The new legislation significantly narrowed the number of government agencies with access to metadata from 80 to 21, a welcome improvement.

Australia's metadata legislation debate did have some interplay with the Snowden revelations. However, it was nothing like Britain's experience.

---

[54] Brandis, G 2014, Speech to the National Press Club Australia https://www.attorneygeneral.gov.au/Speeches/Pages/2014/FourthQuarter2014/1October2014-AddressToTheNationalPressClubCanberra.aspx

[55] AG https://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/26-March-2015-Data-Retention-Bill-passed-by-Parliament.aspx

BULK COLLECTION: BROKEN DEMOCRACY?

In November 2013, roughly ten months before Australia's data-retention legislation was introduced the Australian Broadcasting Corporation (ABC) in partnership with The Guardian reported that Australian intelligence agencies had conducted surveillance on the mobile phone of Indonesian President, Dr Susilo Bambang Yudhoyono. Other targets included the President's wife Kristiani Herawati, as well as others in the President's inner circle[56].

As a result of the report Indonesia recalled its Australian ambassador.[57].

Michael Brissenden was the ABC's Security Correspondent at the time. He took the allegations to the intelligence agencies and the government, which tried to talk him out of publishing. However, the government stopped short of seeking a court-issued injunction, a legal ruling that prohibits the broadcaster or publisher from running the story. This legal option exists for both the Australian and British governments, depending on the circumstances.

Two months after the story was published, the Australian Prime Minister, Tony Abbott denounced NSA whistleblower Edward Snowden as a "traitor" who "betrayed his country". The Prime Minister's criticism of Snowden included an attack on the ABC. Mr Abbott accused the organisation of being "unpatriotic" in its coverage of Snowden and asylum seekers.[58]

[56] Michael Brissenden, 2014 [Online], ABC, Australia spied on Indonesian president Susilo Bambang Yudhoyono, leaked Edward Snowden documents reveal, December 4, 2014 ABC http://www.abc.net.au/news/2013-11-18/australia-spied-on-indonesian-president,-leaked-documents-reveal/5098860

[57] Sydney Morning Herald available online http://www.smh.com.au/federal-politics/political-news/indonesia-recalls-its-ambassador-20131118-2xqb8.html

[58] Bourke L, 2014, Prime Minister Tony Abbott says ABC not on Australia's side in interview with 2GB, Latika Bourke *ABC* February 4, 2014 [Online] http://www.abc.net.au/news/2014-01-29/tony-abbott-steps-up-criticism-of-abc/5224676

Unlike the UK, where the Snowden revelations detailing GCHQ's involvement in bulk data retention reverberated through the courts, the Australian debate was for the most part presented as a response to the rise of Islamic State (ISIL).

Although the threat from ISIL from genuine, Australia's anti-terrorism legislation designed to combat the terrorist threat also included provisions that significantly constrained the press. Each legal provision will be discussed in detail in the anti-disclosure laws section of this chapter.

The initial draft of Australia's metadata legislation arrived without a dataset or safeguards. A review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) added 39 recommendations, including a request for a separate review on the impacts on journalists, the inclusion of a dataset and additional oversight provisions.[59] The government accepted the 39 recommendations in full.

In the UK, the Snowden revelations *not* Islamic State were central to the debate over bulk-data retention. In Australia, the threat of Islamic State was blatantly used as a justification to push through several tranches of anti-terrorism legislation. A mandatory two year metadata-retention scheme was among the many anti-terrorism measures.

Australia's Prime Minister, Tony Abbott along with other politicians routinely used the ISIL terrorism threat as a justification for the introduction of Australia's mandatory bulk-data retention scheme. It's a temptation that former GCHQ Chief Sir David Omand advises against. *"Threats need to be*

[59] Attorney-General for Australia, *The Australian Government has responded to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, March 3, 2015 [online] https://www.attorneygeneral.gov.au/Mediareleases/Pages/2015/FirstQuarter/Government-Response-To-Committee-Report-On-The-Telecommunications-Interception-And-Access-Amendment-Data-Retention-Bill.aspx

explained in ways and at times that distance the dialogue from the pressures of the introduction of legislation or need to justify some new security measure."[60]

[60] Omand D, 2010, *Securing the State,* C. Hurst & Co, London p. 263

The Data Set

Like the UK, the language in Australia's dataset is technology-agnostic, meaning it's legal, not technological, and designed to sustain rapid technological developments.[61]

Telecommunications companies and ISP's in Australia are only now translating the dataset outlined in the 2015 metadata legislation into language understood by engineers.

What is clear is what's not included. The Australian Government is not requiring industry to retain web-browsing history, known in the UK as Internet Connection Records (ICR's). Nor is the content of any emails or phone/internet calls included.

Joss Wright from the Oxford Internet Institute testified before the UK House of Commons Science and Technology Committee when the dataset included in Britain's Investigatory Powers Bill (IPB) was decided. Wright compared the Australian dataset with the UK's.

> *"In many senses it's similar. I think one of the interesting things about the [Australian] dataset is that the definitions stem from concepts used 20, 30 years ago, these are definitions that evolved in the days of the telephone, which landline was used to make a call. The underlying data available has changed and that has led to a world where this is incredibly sensitive information, the data gives a geo-log of your geo locations, which wifi hotspot were you connecting to, who were you with when you were connecting to that wifi hotspot. The datasets in the UK are far more explicit in the IPB in terms of web addresses, there is much more clarity needed in the Australian definitions. "*

(Joss Wright in an interview with the author of this paper, June 2016)

[61] Attorney General of Australia, Dataset description [online] https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/Dataset.pdf

Safeguards

Prior to Australia's mandatory data retention legislation, intelligence and law enforcement agencies could request metadata records without a warrant under the Telecommunications (Interception and Access) Act 1979. Requests were made and accepted on the basis that metadata was required for investigations relating to "criminal offences" or other activities that "threaten safety or security". [62]

A former police officer who worked with metadata said he'd never seen a metadata request turned down on the basis of legitimacy, only for cost issues.[63]

Veteran Australian journalist, Ross Coulthart said a source inside government once showed him his own metadata record and he was shocked.

> *"The source said most requests for metadata aren't made by the Federal Police, rather leak investigations are generally done by the internal security section of each government department."*

(Ross Coulthart in an interview with the author of this paper, May 2016)

Figures detailing how often government agencies access a journalist's metadata are not publically available and unlike the UK IOCCO's report there has been no formal effort to investigate how widespread the practice may have been[64].

---

[62] 2015, Australian Parliament, Senate, Telecommunications (Interception and Access) Amendment (Data Retention) Bill Revised Explanatory Memorandum http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf

[63] 2015, Metadata regime open to abuse, *ABC Download This Show,* Mark Fennell, February 19, 2015 [online] http://www.abc.net.au/radionational/programs/downloadthisshow/6145722

[64] IOCCO 2015, Inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources [online] http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

Journalists interviewed for this paper all felt it was likely that at some point their metadata had been accessed to uncover the identity of a source.

A lengthy battle though Freedom of Information and the Privacy Act revealed the Australian Federal Police (AFP) had in 2014 sought the metadata of Guardian journalist Paul Farrell.[65] This request was made before the data retention bill was passed, when access to a journalist's metadata did not require a warrant. The Guardian reported that the AFP sought the data in pursuit of their journalist's source. The AFP responded by saying the occurrence was "rare". [66] There is no publically available data to prove the claim.

Safeguards designed to ensure state officials don't abuse their access to metadata records were only added as a last-minute amendment to Australia's data retention bill. After much resistance Australia's Prime Minister, Tony Abbott made a reluctant concession to accept some safeguard provisions saying *"The government does not believe that this is necessary but is proposing to accept it to expedite the bill."* [67]

Australia's Attorney-General agreed with the Prime Minister, adding that the safeguards were unnecessary because, *"Australia's existing legal framework is founded on robust principles that provide fair and equal treatment of all subject to its laws."*[68]

---

[65] 2016, Federal Police Admit Seeking access to reporter's metadata without a warrant, Amanda Meade, April 14, 2016 [online] https://www.theguardian.com/world/2016/apr/14/federal-police-admit-seeking-access-to-reporters-metadata-without-warrant

[66] March 2015, Australian Federal Police Commissioner Mark Colvin statement [online] https://www.afp.gov.au/news-media/media-releases/fact-check-use-metadata-relation-journalists

[67] Tony Abbott Gives Ground on Access to Journalists metadata, 16 March 2015, The Guardian [online] http://www.theguardian.com/australia-news/2015/mar/16/tony-abbott-gives-ground-access-journalists-metadata

[68] Ibid.

The safeguards included a warrant that would be required before any of the 21 government agencies could lawfully access a journalist's metadata. A barrister or judge with security clearance would be appointed by the Prime Minister to the position of public interest advocate. The advocate would decide if the 'public interest' in issuing the warrant outweighed the 'public interest' in protecting the identity of the journalist's source.[69]

Australian journalists would *not* be notified if a warrant has been sought nor would they have the right to present their case in front of the Public Interest Advocate.

The journalism trade union in Australia, the Media, Entertainment and Arts Alliance (MEAA) took little comfort from the safeguards. *"Placing a determinant of whether a Journalist Information Warrant will be issued on the secret arguments mounted by Prime Minister-appointed Public Interest Advocates with no media experience or understanding of the public interest in a particular news story is absurd."*[70]

Australia's intelligence agencies ASIO and ASIS would seek access to a journalist's metadata directly via a warrant request to the Attorney-General.

One curious difference between Australia and the UK is that in Australia the requirement for a warrant only applies when a government official requests access to the metadata belonging to a journalist. In the UK's Investigatory Powers Bill any requests seeking to identify or confirm a journalistic source requires a warrant. This means law enforcement agencies in the UK cannot seek a

[69] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 [online] http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375

[70] Media and Arts Alliance, 2016, *Criminalising the Truth, Suppressing the Right to Know, The Report into the State of Press Freedom in Australia*, p. 70 [online] https://www.meaa.org/wp-content/uploads/2016/05/PF_report_2016_HiRes_eBook.pdf

backdoor by mapping the metadata of a suspected leaker and thus avoid seeking a warrant for the journalist's data. This is a subtle but significant difference.

Perhaps the most disturbing clause in the Australian legislation stipulates that should a journalist discover a warrant for their metadata had been sought and subsequently report that fact, they could be liable for a disclosure offence punishable by two years in prison. [71] When coupled with the lack of a deterrent for government officials who might abuse their access to metadata, journalists in Australia have experienced a significant power shift in the direction of the state.

> *"Parliamentary representatives are no longer supporters of protecting against the overreach of the executive or protecting the fundamental freedoms and we've had private admissions that particular parliamentarians didn't read this particular data retention bill, they just wanted to pass it because they saw it as another way of responding to two issues; countering terrorism and child pornography".*

(Australian Human Rights Commission President, Professor Gillian Triggs in an interview with the author of this paper, May 2016)

[71] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, Australia *182A Disclosure/use offences: journalist information warrants*

Oversight

Oversight of Australia's data retention scheme is split across four parliamentary and legal authorities;

1. The Commonwealth Ombudsman is responsible for inspecting the records of enforcement agencies accessing telecommunications data to assess compliance. The Ombudsman will report annually to the Minister but it is unclear if the Minister will make that report public.
2. The Inspector-General of Intelligence and Security will inspect the records of intelligence agencies accessing telecommunications data for compliance.
3. The Information Commissioner will monitor compliance with matters that deal with privacy requirements.
4. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) will inquire into operational matters relating to the use of telecommunications data by Australia's intelligence and law enforcement agencies.

The overwhelming majority of Australian interviewees for this paper felt the oversight mechanisms are neither robust nor transparent enough.

> *"I don't think it's rigorous enough. I think the law leaves a room for a lot of things to go unchecked and I don't think that's a good thing and I don't think it's been tested enough."*

(Michael Brissenden former ABC security correspondent in an interview with the author of this paper, May 2016)

In her many dealings with parliamentary oversight committees President of the Australian Human Rights Commission President, Professor Gillian Triggs observed members tend to approach the issues at hand through a purely partisan prism.

> *"I'm very used to these committees; I give evidence frequently. The questions reflect quite simply a breakdown in political ideology and it's by no means unusual for me to be waiting for the next question while they argue across party lines, correcting each other, making points of order, challenging each others questions. So you get the sense*

> *that this is much less a genuine process of inquiry and understanding than it is a jockeying for position across the two major parties."*

(Australian Human Rights Commission President, Professor Gillian Triggs in an interview with the author of this paper, May 2016)

> *"It's a very unsatisfactory process for an agency head like me to be involved in because it's very hard to engage them in the complexities and to help them understand what they are doing to the rule-of-law and to fundamental freedoms when you're really watching them having this [political] argument when what I'm tying to do is to talk to them about this bill."*[72]

(Australian Human Rights Commission President, Professor Gillian Triggs in an interview with the author of this paper, May 2016)

The next chapter examines how metadata retention interacts with other anti-disclosure legislation in Australia. Those which will be discussed are Section 70 of the Crimes Act, the newly established Border Force Act and a recent amendment to the ASIO Act, Section 35P.

Metadata and disclosure legislation

In Australia both journalists and their sources can be found criminally liable. Whilst sources bear the brunt of anti-disclosure legislation, recent amendments to the ASIO Act could see journalists imprisoned for up to ten years.

In 2010 the Australia Law Reform Commission (ALRC) identified 506 secrecy provisions in 176 pieces of legislation. Around 75% of these offences are punishable by imprisonment for a period exceeding 12 months[73]. With over 500 secrecy provisions one might expect the volume to be offset by relatively high thresholds. Not so. The ALRC found approximately 15% of secrecy provisions relate to the unauthorised disclosure or use of "*any*" information.

Section 70, Crimes Act 1914

Section 70 of the Australian Crimes Act is one such legislative clause. The disclosure offence is broad and includes "any" information or document regardless of the nature of that information[74]. As previously discussed, similar legislation was repealed in the UK in 1972 for being "dangerously broad."[75]

As part of the research for this paper, the Australian Federal Police (AFP) released figures relating to the number of referrals under Section 70 of the Crimes Act. The previously undisclosed data revealed that over the past three years (2013-2015) the Australian Federal Police have received 39 referrals

[73] Australian Law Reform Commission Report Secrecy Provisions 2010, [online] http://www.alrc.gov.au/publications/3-overview-current-secrecy-laws/specific-statutory-secrecy-provisions

[74] Section 70 of the Crime Act [online] http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s70.html

[75] 2015, House of Commons Report, The Official Secrets Act and Official Secrets, December 17, [online] http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7422 p. 15

from Commonwealth departments and agencies to investigate breaches of Section 70. One investigation was referred for prosecution this year.

Financial Year	Number of referrals made
2013/14	11
2014/15	16
2015/16	12
Total	**39**

AFP Figures provided to this paper July 2016. [76]

Once a government department has made a referral, the AFP decides which referrals will be investigated according to internal criteria known as the Case Categorisation and Prioritisation Model (CCPM)[77]. The CCPM model considers:

- Incident type, the impact of the matter on Australian society
- The importance of the matter to both the client and the AFP in terms of the roles assigned to them by Government and Ministerial direction
- The resources required by the AFP to undertake the matter.

The likelihood of a successful prosecution is also a consideration and mandatory metadata increases the chances of a successful prosecution.

The low threshold of Section 70, namely the disclosure of "any" information means that in practice every public servant is breaking the law even when they discuss, with their partner, the simplest

[76] Johnson J (Joanna.Johnson@afp.gov.au) June 21, 2016

[77] Australian Federal Police, Case Categorisation and Prioritisation Model (CCPM) available [online] https://www.afp.gov.au/sites/default/files/PDF/ccpm-may-2010.pdf

details like their day at work. So, when a government official decides to make a referral for investigation it's difficult not to view that referral as politically motivated.

In 2010, The Australian Law Reform Commission recommended that Section 70 be repealed to ensure Australian laws strike *"a fair balance between the public interest in open and accountable government and adequate protection for Commonwealth information that should legitimately be kept confidential."*[78]

Yet Section 70 remains in place and according to AFP figures the law appears to be well in use.

Details on each Section 70 investigation are not available but some information on three notable cases have been reported.

1. National Broadband Network leaks - In May 2016, in the politically-charged atmosphere of a federal election campaign, the Australian Federal Police (AFP) executed a search warrant under Section 70 of the Crimes Act to investigate leaks to the media that discredited the rollout of Australia's National Broadband Network (NBN)[79].

   The police raids were conducted on the offices and homes of Australian Labor Party MPs and staff who were suspected of leaking the confidential documents. Another secrecy provision, Section 79 of the Crimes Act was used to investigate journalists who published stories based on the leaked documents[80].

[78] 2010, Australian Law Reform Commission Report Secrecy Provisions [online] http://www.alrc.gov.au/publications/3-overview-current-secrecy-laws/specific-statutory-secrecy-provisions

[79] The Drum http://www.abc.net.au/news/2016-05-26/bradley-we-should-be-worried-by-how-the-afp-wields-its-power/7446888

[80] Redacted online version of the NBN search warrant http://www.abc.net.au/mediawatch/transcripts/1617_warrant.pdf

2. Nauru Doctor - In April 2016, Australian psychiatrist Dr Peter Young revealed that he was the subject of an AFP investigation under Section 70 of the Crimes Act after he spoke to the ABC in December 2014 and April 2016 about the death of an asylum seeker, Hamid Kehazaei on Australia's Manus Island detention centre[81].

   Dr Young used the Privacy Act to request access to files held on him by the AFP. The heavily redacted files show Dr Young was the subject of an investigation as a result of "comments attributed to him being highly critical of [the immigration department] and [service provider] IHMS in their handling of asylum seeker medical care" in two news reports.

3. Save the Children workers - In October 2014, Australia's then Immigration Minister Scott Morrison, referred a number of Save the Children employees to the Australian Federal Police for investigation relating to disclosure offences under Section 70 of the Crimes Act.

   Save the Children, an aid development NGO was contracted by the Australian Government to provide services to refugees and asylum seekers housed in Australia's system of offshore detention centres, in this case on the Pacific Island nation of Nauru.

   The workers were accused of breaching Section 70 when they submitted a detailed submission to the Human Rights Commission detailing allegations of sexual and physical abuse of children.[82]

[81] May 23, 2016, Australian Police Access Phone Records of Aslyum Whistleblower, The Guardian http://www.theguardian.com/australia-news/2016/may/24/australian-police-accessed-phone-records-of-asylum-whistleblower

[82] 2015, Doherty B, *The Guardian*, Police Investigate Save the Children whistleblowers, March 4, 2015 http://www.theguardian.com/australia-news/2015/mar/04/police-investigate-save-the-children-whistleblowers-over-nauru-abuse-report

> During this time, leaks about immigration detention appeared to be coming from both inside the Nauru detention centre but also from inside government. The Daily Telegraph newspaper referenced a government 'intelligence report' which they claimed revealed Save the Children staff had coached asylum seekers to self harm. [83] Intelligence reports from Australia's offshore detention centres are not publically available. The apparent government leak was never referred for investigation under section 70. Instead, the government only chose to pursue alleged unauthorized disclosures by Save the Children Staff.

This example not only demonstrates the willingness of the government to use Section 70 to track down and prosecute a journalist's source, but also reveals a willful blindness when the law is not equally applied.

> *"The government says to us, 'well look there are no prosecutions, it's rarely ever used, only extreme cases', but that's not really true and they would have gone for Save the Children if they could have done, and they are still vulnerable so this is still an open issue. The existence of the secrecy provisions has a very big chilling effect on anyone who wants to speak out and certainly for journalists."*

(Australian Human Rights Commission President, Professor Gillian Triggs in an interview with the author of this paper, May 2016)

Veteran Australian journalist Ross Coulthart has been told by his sources inside government that leak investigations happen at the departmental level and almost always involve metadata. As a result he's concerned about the potential for abuse under Australia's mandatory data retention scheme.

---

[83] 2014, Simon Benson and Jennifer Rajca, *The Daily Telegraph*, Truth Overboard Claims of Aslyum Seeker Abuse on Nauru Were Fabricated, October 3, 2014 [online] http://www.dailytelegraph.com.au/news/nsw/truth-overboard-claims-of-asylum-seeker-abuse-on-nauru-were-fabricated/news-story/cbe8350e21ebd8d3a17d39d53e121c59

> *"And now we throw the key to the safe and assume our metadata is safe because the good people in [government] and our intelligence services would not use it for bad motives, give me a break."*

(Ross Coulthart in an interview with the author of this paper, May 2016)

Border Force Act, 2015

In 2015 the Australian parliament passed another low threshold anti-disclosure law as part of the Border Force Act.[84]

Under the Act, government employees or contractors who disclose information, not classified information or information that could be proven to damage the state, just general information about Border Force operations could face two years in prison.

Since the introduction of the Border Force Act, doctors, physicians and workers from Australian detention centres have in protest dared the government to prosecute them by continuing to speak to the press about conditions inside Australia's detention centres. [85]

AFP confirmed to the author of this paper that there have been no referrals for disclosure under the Border Force Act.

---

[84] Australian Border Force Bill 2015 [online] http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5408

[85] June 30, 2015 Open Letter to the Border Force Act: 'We Challenge the Department to Prosecute' [online] http://www.theguardian.com/australia-news/2015/jul/01/open-letter-on-the-border-force-act-we-challenge-the-department-to-prosecute

Those accused of breaching both Section 70 of the Crimes Act and the Border Force Act are entitled to a public interest defence under the 2013 Public Interest Disclosure Act[86].

However, this legislation has been criticised as excessively onerous for whistleblowers[87]. Protection from criminal liability only applies to external disclosure, if the disclosure has first been made internally with the exception of an emergency. Emergency is regarded as imminent danger to the health or safety of one or more persons and does not cover intelligence information.

The disclosure must also meet the various thresholds of 'disclosable conduct', defined as conduct that is 'illegal, corrupt, perverts the course of justice' or involves an 'abuse of public trust'. [88] If the 'disclosable conduct' takes place related to a foreign country the disclosure is only protected if the conduct is illegal in that country.[89]

In their analysis of the 2013 Public Interest Disclosure Act, Liberty Victoria concluded it would be "extremely difficult" for a whistleblower to be confident they have fulfilled all of the threshold requirements before making the disclosure.[90]

[86] Public Interest Disclosure Act 2013, Australian Government [online] https://www.legislation.gov.au/Details/C2013A00133

[87] Liberty Victoria, 2016, *Operation Secret Borders: What we Don't Know Can Hurt Us*, Liberty Law Reform Report, 16 April 2016

[88] Ibid p. 36

[89] Ibid

[90] Ibid. p 43

Section 35P of the ASIO Act

A few months before Australia's proposed data retention scheme was announced a disclosure amendment to the ASIO Act dramatically altered the balance of power between journalists and the government.

In 2014, an amendment to the ASIO Act, Section 35P, made disclosing information relating to a Special Intelligence Operation (SIO) an offence punishable by five years in prison. The aggravated offence, punishable by ten years in prison, occurs when the disclosure endangers the health or safety of any person or prejudices the SIO, or where the person intends such results.[91]

The legislation took a total of six weeks to pass though parliament.[92]

The law covers *all aspects* of an SIO operation, *all of the time*, long after those operations have ceased[93].

If a civilian was killed or tortured in an SIO, Australians would never know about it – not even years after that operation had ceased. Section 35P ensures SIO's would never be reported regardless of the public interest, for which there is no defence.

Unlike the active DA-Notice system in the UK, an informal mechanism whereby journalists can seek guidance about stories that may damage national security or trip-up an intelligence operation, the D-Notice system in Australia became defunct in the 1990's. Whilst not formally abolished, the

[91] Hardy K, Williams G, 2016 *AusLaw,* Australian legal Responses to Foreign Fighters

[92] National Security Legislation Bill (1) 2014 http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s969

[93] ASIO Act 35P amendment [online] https://www.legislation.gov.au/Details/C2015C00105/Download

Independent National Security Monitor Roger Gyles noted it appeared to have "informally collapsed"[94].

Section 35P of the ASIO Act was not well received by the Australian media. In an effort to quell the backlash Australia's Attorney General gave this assurance. *"There is no possibility, no practical or foreseeable possibility that in our liberal democracy a journalist would ever be prosecuted for doing their job".*[95]

Yet 35P remains in place with the full punishment penalty of up to 10 years in prison. It's difficult to see how the Attorney can offer such a blanket assurance.

> *"I think it is very misleading for a PM or an attorney to use the broad language of a liberal democracy that the protections are available in our constitution when they manifestly are not"*[96]

(Australian Human Rights Commission President, Professor Gillian Triggs in an interview with the author of this paper, May 2016)

At the time, veteran political journalist Laurie Oakes spoke out deriding the new laws, making the point that if the Attorney-General truly believed a journalist would never be prosecuted then why wasn't a public interest or good faith defence drafted into the legislation?

---

[94] The Independent National Security Legislation Monitor (INSLM), *2015 Report on the impact on journalists of section 35P of the ASIO Act*

[95] October 30 2014, George Brandis: attorney general must approve prosecution of journalists under security laws http://www.theguardian.com/australia-news/2014/oct/30/george-brandis-attorney-general-approve-prosecution-journalists-security-laws

> *"If the government was fair dinkum in its claims that 35P is not directed at journalists, it's very hard to see why an exemption of that kind would not be acceptable".*[97]

The backlash sparked an almost immediate review of 35P by Australia's Independent National Security Monitor, Roger Gyles QC. Mr Gyles found the law to be "*arguably invalid"* on the basis that it is inconsistent with Australia's obligation to provide freedom of political communication in accordance with Article 19 of the *the International Covenant on Civil and Political Rights*. [98].

Mr Gyles QC did not recommend a public interest test, arguing the judiciary *"should not lightly be involved in binding value judgments about issues of national security"*[99].

Instead, Mr Gyles recommended the liable thresholds be lifted. He recommended a person or journalist should only be liable for five years in prison if the reporter was aware the SIO disclosure carried *'substantial risk'* of endangering the health or safety of those involved or would prejudice the intelligence operation. To attract the ten-year punishment, the journalist would have *'knowledge'* that reporting on an SIO would endanger health and safety or harm the conduct of an operation. [100]

Almost one year on, Mr Gyles' recommendations are yet to be put to parliament.

In reviewing the recommendations, lawyers with the Media, Entertainment and Arts Alliance (MEAA) along with constitutional lawyer, George Williams noted the improvements but added they did not

---

[97] Oakes L, *Press Freedom Speech* 2015 Melbourne [online] https://pressfreedom.org.au/media-got-complacent-637c55497363#.3luw3myic

[98] Gyles R, 2015 *Independent National Security Legislation Monitor, Report on the impact on journalists of section 35P of the ASIO Act* [online] https://www.dpmc.gov.au/sites/default/files/publications/inslm_report_impact_s35p_journalists.pdf

[99] Ibid.

[100] Ibid.

remedy the fundamental problem with the legislation insofar that 35P criminalises journalists who report on matters that may be in the public interest[101].

Australian investigative journalist Ross Coulthart is adamant that the effect of 35P is clear, stories in the public interest will never see the light of day.

> *"What say we'd loaned a couple of Australians to the C.I.A's extraordinary rendition program because Australian accents are less suspicious than American, and what say, a couple of backpackers in a European country turned out to be SAS soldiers on secondment from Australia's military? Should that story be told, what do you think?"*

(Ross Coulthart in an interview with the author of this paper, May 2016)

When governments are seen to manipulate terrorism threats by introducing responsive measures that constrain a free press, as 35P does, trust in governments is eroded. The assurance made by Australia's Attorney-General George Brandis QC, that no journalist would ever be jailed in our 'liberal democracy' is disingenuous, as the law clearly affords the state the option. The decision to prosecute, therefore, is political.

[101] MEAA, 2016 *Criminializaing the Truth Supressing the Right to Know, Report into the State of Press Freedom in Australia 2016* [online] https://www.meaa.org/wpcontent/uploads/2016/05/PF_report_2016_HiRes_eBook.pdf

Conclusion

At the time of writing, journalists in the UK and Australia were afforded similar safeguards under their respective mandatory data retention regimes. Both systems require warrants before access to communications data is granted.

It's worth remembering this paper was written as the UK's Investigatory Powers Bill (IPB) was in the final throes of parliamentary debate and the possibility for change in its final form is real. During this time, the UK voted to leave the European Union and Theresa May succeeded David Cameron as Britain's Prime Minister. As a result of these seismic changes, there is a possibility that Britain will withdraw as a signatory to the European Convention on Human Rights, a move that would have an unpredictable impact on the issues discussed in this paper.

But as the IPB stands, journalists in the UK have lost ground. Under the PACE provisions journalists were notified when a warrant was sought on their metadata and they were afforded the right to argue against the warrant in front of a judge. That has been lost in the Investigatory Powers Bill, a serious diminution of conditions.

Journalists in Australia gained ground, albeit it from a very low base. But when the broader picture is considered, a new paradigm emerges - that of mandatory data retention coupled with low threshold anti-disclosure laws. This unique legal environment is particular to Australia and not replicated in the UK. In the 1980's Britain repealed its "catch-all" disclosure laws after the Franks report found them to be "enormously wide" and not befitting of British democracy because they impinged on the freedom of information.

By contrast, Australia has a sizeable and increasing array of low threshold or catch-all disclosure laws. Many of them carry criminal liability of up to ten years in prison. Recent cases demonstrate these anti-disclosure laws are being applied unequally and for political ends.

Examples of Ericson's 'counter-law' are easily identifiable in Australian legislation, including Section 70 of the Crimes Act and Section 35P of the ASIO Act. Despite assurances to the contrary by politicians, traditional rule-of-law principles have been eroded.

These encroachments might contribute to a mood of injustice and inspire leaks, the very thing the government is trying to occlude.

In Australia, the debate over data retention was overwhelmed by politically driven alarm over the rise of Islamic State. The government offered the false assumption that by suspending human rights, security would be assured. It was an episode of poorly disguised sophistry and executive overreach.

In contrast, debate in the UK focused on the fundamental question of how to legislate for state surveillance without eroding rule-of-law principles.

Kicked off by the Snowden revelations, debate in the UK over bulk collection was largely shaped by legal battles. Precedents were drawn and set the bounds for what was acceptable in a democracy that enshrines civil rights, namely the right to freedom of expression.

Consequently, the debate was more granular and safeguards and oversight provisions were taken more seriously. However, when Theresa May gave assurances that the IPB would come with the most robust safeguards in the democratic world, she stopped short of saying in the 'liberal' democratic world. And that should be the measure.

Journalists in the UK have lost ground in the proposed Investigatory Powers Bill. Their capacity to protect the identity of a source has been diminished if not removed. Journalists in Australia are in the same predicament, however the compounding effect of low threshold disclosure laws poses a very serious threat to a free press and the liberal nature of Australia's democracy.

In their examination of liberal democracies Sharun Mukand and Dani Rodrik concluded that the surprise is not that few democracies are liberal, but that liberal democracies exist at all. Achieving an

acceptable balance between preserving the 'liberal' nature of our democracies whilst providing security for citizens may prove elusive. What is clear is that journalists will feel the effects first and most acutely.

Bulk data collection regimes have compromised the core principle of source confidentiality and when combined with low threshold anti-disclosure laws the free flow of information is threatened.

If Australia and the UK are truly committed to a free press, a defining characteristic of a liberal democracy, then now in this era of bulk data collection, governments could prove the veracity of their rhetoric and enshrine that right.

BIBLIOGRAPHY

Anderson D, *A Question of Trust: Report of the Investigatory Powers Review,* June 2015 [online https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

Attorney-General for Australia, *The Australian Government has responded to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, March 3, 2015

Austin L, (2015) Lawful Illegality: What Snowden has Taught us about the legal infrastructure of the Surveillance State, In: (eds.) Michael Geist, Law Privacy and Surveillance in Canada in the post-Snowden Era, Canada, University of Ottawa Press.

Australian Federal Police, Case Categorisation and Prioritisation Model (CCPM) available [online] https://www.afp.gov.au/sites/default/files/PDF/ccpm-may-2010.pdf

Australian Parliamentary Joint Committee on Intelligence and Security *Inquiry into the authorisation of access to telecommunications data to identify a journalist's source*, March 4, 2015

Australian Law Reform Commission Report Secrecy Provisions 2010, [online] http://www.alrc.gov.au/publications/3-overview-current-secrecy-laws/specific-statutory-secrecy-provisions

BBC 2013, David Cameron criticises the Guardian for publishing Snowden data, October 16, 2013 *BBC* [online] http://www.bbc.co.uk/news/uk-politics-24555955

BBC 2015, GCHQ censured over sharing of internet surveillance data with US, *BBC* February 6, 2015 [online] http://www.bbc.co.uk/news/uk-31164451

BBC 2013, David Miranda Detention: MP asks police for explanation, *BBC,* August 19, 2013[online] http://www.bbc.co.uk/news/world-latin-america-23750289

Brooke H, The Silent State: Secrets, Surveillance and the Myth of British Democracy

Bobbitt P, 2008, *Terror and Consent: the wars of the 21st Century*, Alfred A. Knopf, a division if Random House, New York

Boehm, F Hert P 2012 *Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law,* European Journal of Law and Technology, Vol. 3, No. 3

Bowling, B. and Sheptycki, K. 2015 *Global Policing and Transnational Law Enforcement King's College London Dickson Poon School of Law Legal Research Paper Series,* Paper No. 2015-10. London: Sage

Bowling, B. and Sheptycki, K. (2015) *Global policing and transnational rule with law* Transnational legal Theory Jun 6:1

Brandis, G 2014, Speech to the National Press Club Australia [online] https://www.attorneygeneral.gov.au/Speeches/Pages/2014/FourthQuarter2014/1October2014-AddressToTheNationalPressClubCanberra.aspx

Corera G, 2016, *Intercept: The Secret History of Computers and Spies,* London, Weidenfeld & Nicolson

David Miranda vs. Home Office Met Police UK Court of Appeals, January 19, 2016 https://www.judiciary.gov.uk/wp-content/uploads/2016/01/miranda-v-home-sec-judgment.pdf

Draft Investigatory Powers Bill, UK Cm 9152, November 2015, [online] https://www.gov.uk/government/publications/draft-investigatory-powers-bill

Ericson, Richard V. 2008, *Risk and the War on Terror,* London Taylor and Francies

Ericson, 2007, *Crime in an Insecure World*, United Kingdom, Polity Press Cambridge

Freedom House 2016, *Press Freedom Index*, [online] https://freedomhouse.org/report/freedom-press/freedom-press-2016

Johnston T S. 2014 The Snowden revelations: Is GCHQ breaking the law*? European Human Rights Law Review*

Gyles R, 2015 *Independent National Security Legislation Monitor, Report on the impact on journalists of section 35P of the ASIO Act* [online] https://www.dpmc.gov.au/sites/default/files/publications/inslm_report_impact_s35p_journalists.pdf

Haggerty K.D, Samatas, 2010, *Democracy and Surveillance,* London Routledge

Interception of Communications Commissioner, *Half-yearly report*, HC 308, 16 July 2015

Interception of Communications Commissioner, *Inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources*, February 4, 2015

Kühling J, Heitzer S 2015 Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24 in the UK and elsewhere *European Law Review*

Liberty Victoria, 2016, *Operation Secret Borders: What we Don't Know Can Hurt Us*, Liberty Law Reform Report, 16 April 2016

Media and Arts Alliance, 2016, *Criminalising the Truth, Suppressing the Right to Know, The Report into the State of Press Freedom in Australia*.

Moran C., 2013, *Classified Secrecy and the State in Morden Britain,* Cambridge University Press United Kingdom

Mukand S, Rodrik D, 2015 The Political Economy of Liberal Democracy, Working Paper available at Working Paper 21540 [online] http://www.nber.org/papers/w21540

Oakes L, *Press Freedom Speech* 2015 Melbourne [online] https://pressfreedom.org.au/media-got-complacent-637c55497363#.3luw3myic

Ojanen T, 2014 Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance *European Constitutional Law Review*

Omand D., 2010, *Securing the State,* C. Hurst & Co, London p.265

Orwell G 1956, Politics of the English Language, in his *Collections of Essays,* New York, Harcourt Brace Jovanovich

Reiner, R. 2000, *The Politics of the Police*, Oxford University Press, New York

RUSI Report *A Democratic Licence to Operate: Report of the Independent Surveillance Review* July 13, 2015 [online] https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review

Theresa May Investigatory Powers Bill Speech [online] November 4, 2015 [online] https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

UK House of Commons Briefing *Access to Journalists' Sources*, No. 07440, 31 December 2015 p. 5

UK Home Office Impact Assessment Oversight, Investigatory Powers Bill 2015 [online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473777/Impact_Assessment-Oversight.pdf

UNESCO Report World Trends in Freedom of Expression and media Development, Ch. Protecting a journalists source 2015

Zakaria F, 1997 *The Rise of Illiberal Democracy* Foreign Affairs, November/December issue