INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 1

The passage of Australia's data retention regime: national security, human rights, and media scrutiny

Nicolas Suzor
School of Law, Queensland University of Technology, Brisbane, Australia, n.suzor@qut.edu.au

Kylie Pappalardo
School of Law, Queensland University of Technology, Brisbane, Australia, k.pappalardo@qut.edu.au

Natalie McIntosh
School of Law, Queensland University of Technology, Brisbane, Australia, natalie.mcintosh@connect.qut.edu.au

Published on 14 Mar 2017 | DOI: 10.14763/2017.1.454

Abstract: In 2015, the Australian government passed the Telecommunications (Interception and Access) Amendment (Data Retention) Act, which requires ISPs to collect metadata about their users and store this metadata for two years. From its conception, Australia's data retention scheme has been controversial. In this article we examine how public interest concerns were addressed in Australian news media during the Act's passage. The Act was ultimately passed with bipartisan support, despite serious deficiencies. We show how the Act's complexity seemed to limit engaged critique in the mainstream media and how fears over terrorist attacks were exploited to secure the Act's passage through parliament.

Keywords: Data retention, Human rights, Media, Metadata, Security, Public interest

Article information

Received: 19 Jun 2016 **Reviewed:** 06 Feb 2017 **Published:** 14 Mar 2017

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/passage-australias-data-retention-regime-national-security-human-rights-and-media

Citation: Suzor, N. & Pappalardo, K. & McIntosh, N. (2017). The passage of Australia's data retention regime: national security, human rights, and media scrutiny. *Internet Policy Review*, *6*(1). DOI: 10.14763/2017.1.454

This paper is part of Australian internet policy, a special issue of Internet Policy Review *guest-edited by Angela Daly and Julian Thomas.*

PART I: THE DATA RETENTION ACT

In April 2015, the Australian government passed the *Telecommunications (Interception and Access) Amendment (Data Retention) Act*, which requires Internet Service Providers (ISPs) and telecommunications providers to store information about their subscribers' online activity for a period of two years. The data retention rules apply to metadata – loosely defined as information that is not the 'content' of a communication. Generally, service providers must keep identifying information about their subscribers, including billing information, and information about the type, time, duration and location of communications. The act excludes much internet activity and web browsing history. Information must be stored for two years for most information and must be encrypted and stored securely. The act enables approved law enforcement agencies to access this data without a warrant, except for the specific case of data relating to journalists.

The final text of the act is complex, confusing, and lacks key safeguards to protect the privacy of Australians. In part II of this article, we review the obligations imposed by the act and the mechanisms that have been introduced to protect human rights. Experience from other jurisdictions and the recommendations of Australian reviews suggest that mass data retention obligations can only be justified if they are clearly necessary and curtailed to limit access to data for the purposes of addressing serious crimes with full judicial oversight. The act, as passed, does not contain these safeguards, and important terms are not defined in the act or are defined only in the negative or in explanatory materials.

Public interest concerns were raised consistently throughout the period in which the bill was under consideration, but were ultimately not directly addressed by the government. In part III, we review the history of the act's introduction as represented in the Australian press media, in order to better understand how the act was passed without resolving these core human rights tensions. The final text of the act reflects the trauma the government suffered during its passage, resulting in a number of very specific limitations that address the most acute and politically problematic concerns raised by opponents. The larger-scale concerns about the necessity of introducing mass-scale surveillance obligations or the scheme's uncertain scope, vague specification of access rights, and limited judicial oversight, however, were not well represented in the media. Our analysis suggests that the government was able to exploit the complex and uncertain scope of the data retention obligations in its favour to marginalise opposition that hinged on quite technical questions of coverage and access. The government was also able to draw heavily on escalating national security rhetoric around several high-profile terrorist attacks to effectively sidestep scrutiny about why the new obligations were required. Ultimately, while the government had to make several concessions to particular interest groups, it was able to avoid substantively addressing key concerns about the scheme in the media by channelling attention to the more easily answered question about whether the proposed data set would be included in the legislation. Many of the issues raised during the passage of the act were effectively deferred to be resolved at a future date, either by a review committee or through ministerial regulations, giving the government the time it needed to secure bipartisan support for its passage.

PART II: NECESSARY AND PROPORTIONATE

The data retention act introduces highly complex obligations and a set of outstanding issues that

have not fully been resolved. In this part, we consider some of the key issues with the act from the perspective of the human right to privacy, generally represented in international documents as the right not to be subjected to arbitrary interference with privacy, family life, home and correspondence (UDHR 1948, Art 12; ICCPR 1966, Art 17; CFREU 2000, Art 7). According to international human rights law, in order for a data retention regime to be legitimate, it must be both necessary to address a legitimate goal and be a proportionate means to achieving that goal. In this part, we argue that the government has not discharged its burden of showing that Australia's data retention obligation is a necessary measure, and that it has not been appropriately tailored to satisfy the requirements of proportionality.

Australia's data retention scheme comes during a period of great international scrutiny of indiscriminate surveillance regimes (Brown et al., 2015). Edward Snowden's revelations of the extent of surveillance of global internet traffic captured by the Five Eyes alliance (of which Australia is a member) have fuelled intense concern about how the technical capabilities of intelligence and law enforcement agencies can be limited in a way that ensures individual liberties are adequately protected (Greenwald, 2014).

Opinions differ as to whether and how a metadata retention scheme can be compatible with freedom of expression and privacy rights. The strongest statements, like the 'necessary and proportionate' (2014) principles developed by a coalition of civil rights societies, academics and privacy and technology experts, prohibit completely the indiscriminate collection of metadata. The UN and Inter-American Special Rapporteurs on Freedom of Expression (2013) have warned that access to telecommunications data should only be authorised under the 'most exceptional circumstances'. The European Court of Justice (ECJ) has held that an indiscriminate data retention obligation went beyond what was necessary and proportionate to achieve its objectives to fight 'serious crimes' and was therefore incompatible with the fundamental right to privacy and to data protection (*Digital Rights Ireland v Minister for Communications*, 2014). Similar to the Australian scheme, the European Directive 2006/24/EC required providers of publicly available electronic communications services or public communications networks to retain 'traffic and location data' – though not 'the content of electronic communications' – for periods between six months and two years (articles 2, 5, 6). The object of the directive was to ensure that data was available for the investigation, detection and prosecution of serious crime, including acts of terrorism (article 1; *Digital Rights Ireland* [41]-[42]). The ECJ found that fighting serious crime and international terrorism to maintain international peace and security was an objective of general interest (*Digital Rights Ireland* [41]-[42]). However, given that the directive's interference with the right to privacy was 'wide-ranging', 'serious' and likely to make people feel as though their private lives were subject to constant surveillance ([37]), the data retention had to be proportional and strictly necessary to achieve this objective. The ECJ held that it was not. In so holding, the court focused in particular on the fact that the scheme would affect *all* persons using electronic communications services, regardless of their connection to criminal activity ([58]); that the directive contained no objective criteria by which to determine the limits of the access and use of retained data by competent national authorities in detecting, preventing or prosecuting serious crime ([60]); that the directive did not provide for prior review by a court or independent administrative body ([62]); and that there were insufficient safeguards to ensure the effective protection of retained data against the risk of abuse or unlawful access ([66]). [1] As we highlight below, Australia's own data retention act shares these same shortcomings.

In the United States, a presidential review of surveillance recommended that access to data must be strictly limited to national security interests and permitted only with a court order (Review

Group on Intelligence and Communications Technologies, 2013). In the US, where warrantless access to metadata about citizens' behaviour raises serious legal and constitutional concerns (Donohue, 2014), a Presidential Policy Directive (2014) requires even surveillance targeted at non-US persons to be used only in relation to national security, cybersecurity, and transnational crime. While it is hard to articulate a definitive standard as to when data retention regimes will be proportionate (Brown et al., 2015), a minimal baseline seems relatively clear: measures that are justifiable on national security grounds may not be justifiable for ordinary law enforcement purposes, and access to metadata must be constrained by legitimate judicial authority. In this part, we review Australia's new data retention obligations against these standards.

A. SCOPE OF OBLIGATIONS

The scope of data that is required to be stored by telecommunications providers and internet service providers is not clearly defined in Australia's act. The act requires service providers to store identifying information about the subscriber, their billing information, address, and account details; the source, destination, time, and duration of communications; the type of communication or service used by the subscriber, such as voice, SMS, email or social media (for the type of communication) or Wi-Fi, VoIP or cable (for the type of service); and location information at the start and end of communications (s 187AA(1)). This list can be changed at any time by ministerial declaration, though a declaration is deemed to be in force only for 40 sitting days of parliament (s 187AA(2),(3)).

From this broad list of information, several distinct categories are excluded. The most important of these is that the 'contents or substance of a communication' is not required to be stored (s 187A(4)(a)). The legislation also excludes details about what subscribers access over the internet – service providers are not required to capture IP addresses of connections users make online and other information that relates to services provided by third parties (called 'over the top' services) (s 187A(4)(b),(c)). The complex way that 'over the top' services are excluded creates an unusual distinction in the Act where services that are provided by Australian ISPs themselves will actually be included within the scope of the obligation. So, for example, if a subscriber accesses email through a third party provider, like Google, or makes a call through a VoIP service like Skype, these are 'over the top' services, and the provider is under no obligation to retain any information about their use. But, where email or VoIP services are provided by the ISP itself, it is required to store any information about the communications its users make – including addresses to which emails are sent or calls placed. The situation is further complicated by the fact that the providers to whom data retention obligations apply can be expanded by declaration at a later date (s 187A(3B)) – which means that the minister or an authorised person may require Australian service providers, including website hosts, company intranets, discussion forums, and other online services, to store data about their use.

The obligations imposed for mobile and fixed telephony communications are more extensive than those imposed for internet traffic. Telecommunications providers are required to store details about connections to the network and information about calls and messages sent over the network. Information that is not 'content', in this respect, includes the number dialled or the recipient of an SMS; the duration of a call; and the location of a mobile phone user at the start and end of the call. The act excludes location information about a telecommunications device where that information is not used by the service provider in providing the relevant service (s 187A(4)(e)) – for example, there is no obligation to store the reported GPS coordinates of a mobile phone, only the location of the cell towers the phone is connected to.

B. ACCESS TO METADATA

The broad scope of the Australian data retention regime raises a clear potential conflict with the human right to privacy. The regime requires indiscriminate capture of an extensive set of information that reveals important details of private communications - information that is itself private. Given the broad obligations to retain communications data, the question of access becomes crucial. Under previous law, a broad range of government agencies have been able to access data held by telecommunications providers in the course of enforcing a criminal law or imposing a monetary fine (*Telecommunications Interception and Access Act 1979* (Cth), ss 178, 179). The list of bodies that routinely use this power is relatively large, and includes local councils, animal welfare organisations, Australia Post, and various federal and state departments (Attorney-General's Department, 2015). The *Data Retention Act* introduces a list of criminal law-enforcement agencies that is substantially narrower than the diverse organisations that were previously accessing data, and includes police services, crime and corruption commissions, customs, the Australian Securities and Investment Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) (s110A(1)).

While the act, as introduced, appears to limit the bodies that are empowered to access telecommunications data without a warrant, the list can be modified by ministerial declaration. Documents obtained through freedom of information requests in January 2016 indicate that 61 different bodies had so far applied for ongoing access to telecommunications data (Guy, 2016). This list represents a very diverse range of organisations, again including many government departments, some local councils, and a broad range of state and federal regulators. No declaration has been made as yet as to which of these requests will be authorised, although reportedly the Attorney-General's Department has rejected at least one application - that of Australia Post, which sought access to metadata to track mobile phones stolen from the company's retail stores (Taylor, 2016).

C. HUMAN RIGHTS SAFEGUARDS

The potentially broad and as yet unknown list of agencies that are able to access telecommunications data without a warrant is concerning. Whether Australia's data retention scheme is proportionate essentially rests on the extent to which it is curtailed to achieving a legitimate purpose. The government has consistently justified the data retention scheme to the Australian public on the basis that it is vital to assist in national security investigations and matters of serious crime. The risk posed by the act, however, is that the massive volume of data that is requires to be created and maintained will, once it exists, be open to access by a wide range of bodies for a wide range of other purposes, without the judicial oversight that a warrant would require.

These concerns were raised by the Parliamentary Joint Committee on Human Rights (PJCHR) in its review of the scheme. The committee concluded that the government had not yet clearly demonstrated that the obligation to store data for two years was necessary (PJCHR, 2014). This hurdle is important, given that Australia already has a data preservation scheme, enacted in 2012. The *Cybercrime Legislation Amendment Act* ratified Australia's accession to the Council of Europe Convention on Cybercrime and introduced a scheme to permit law enforcement agencies to require carriage service providers to preserve communications data for specified persons in relation to both domestic and foreign investigations. The government has provided no clear explanation as to why this existing data preservation scheme was inadequate.

Even assuming the scheme was necessary, the lack of judicial oversight over which agencies can access data and for what purposes is concerning. The government, in asserting that the act

complies with human rights standards (Explanatory Memorandum, 2015), relies on the procedural safeguards in the decision as to whether to grant an organisation's request to become an authorised agency. These safeguards require the minister to consider a range of issues, including whether the organisation is likely to protect the information it receives and whether the declaration would be in the public interest. Ultimately, however, the scope for ministerial discretion is relatively large in this regard, and many of the bodies that have previously accessed telecommunications data would potentially be able to satisfy the test under the new legislation. There is accordingly good reason to suspect that in operation, Australia's data retention scheme will be used not just for the purpose of investigating serious crimes and national security matters, but also for a wide range of much more minor criminal offences and regulatory penalties.

The other safeguard the government points to in justifying the scheme is that the act requires reporting mechanisms. The act requires agencies that access telecommunications information to keep records and make annual reports detailing the number of times that the agency accessed telecommunications information during that year. These reports are then tabled before parliament (ss 186, 186A). Additionally, the Commonwealth Ombudsman is given power to inspect the records kept by agencies, and is likewise under a responsibility to report to the minister each year about these inspections. Again, the minister must table the ombudsman's report in parliament. A separate provision requires the minister to make an annual written report on the operation of the data retention scheme.

While reporting after access is important for parliamentary oversight, it is no substitute for judicial oversight before access to information. The PJCHR recommended that a warrant be required for access to metadata, and that access be limited to investigations of serious crimes. It considered that the act's oversight mechanisms were insufficient, in that they only required reporting on access powers after they had already been exercised and after a person's privacy had been violated (Parliamentary Joint Committee on Human Rights, 2014).

Ultimately, the concerns raised by the PJCHR were mostly rejected by the government. In his response to the PJCHR, the Attorney General disagreed with the 'suggestion' that agencies be required to obtain a warrant to access metadata. Minister Brandis argued that a warrant requirement would be 'impractical', noting, 'Warrant applications take considerable time to develop, which necessarily delays investigations and creates a risk that perishable physical, electronic and testimonial evidence will be lost' (PJCHR, 2015, p. 66).

In light of the large scope of Australia's data retention obligations, widespread potential use, and lack of judicial oversight, it seems difficult to accept that the government has sufficiently demonstrated that it is a necessary and proportionate response. Importantly, Australia's act contains all of the same weaknesses that rendered the European Directive 2006/24/EC an unacceptable interference with the right of privacy in the *Digital Rights Ireland* decision outlined above (*Digital Rights Ireland v Minister for Communications*, 2014). In introducing and justifying the act, the Australian government relied heavily on rhetoric surrounding increasing threats to national security and the need for more efficient criminal investigation for serious crimes. Even assuming that the legislation is necessary on these grounds, its operation is not limited to serious crimes. Most particularly, in its response to the PJCHR, the government has not given a convincing explanation that agencies investigating more minor crimes or regulatory fines might need access to telecommunications data without a warrant. In the remainder of this article, we consider how the government was able to reject these human rights concerns in securing the passage of the act.

PART III: THE PUBLIC INTEREST AND THE POLITICAL PROCESS

In this part, we proceed from the position that civil society has an interest in ensuring that laws imposing surveillance are necessary and proportionate to the harm that they are trying to prevent. With this in mind, we examine what went wrong with the Australian data retention scheme. The concerns with the act discussed in the previous part were all raised by journalists, cross-bench senators, and public interest groups throughout the entire period of the act's introduction. The act was introduced during a period of great global hostility to government surveillance following Edward Snowden's revelations of the extent to which the United States National Security Agency (NSA) and its Five Eyes allies were able to capture internet data. The European Court of Justice had only months previously rejected as violating EU law the scheme upon which the Australian Bill was explicitly based (*Digital Rights Ireland v Minister for Communications*, 2014). The government's introduction of the act was bungled, in that neither the Prime Minister nor the Attorney General could explain what 'metadata' meant, and the government continually struggled to articulate the justifications that made its introduction necessary. From the time at which its introduction was first mooted, opinion polls showed that over half of Australians surveyed opposed the act (Murphy, 2014).

The fact that the act was passed with only minor concessions to the public interest concerns in these circumstances suggests a clear limitation in the ability of civil society to influence Australian law making. This is deeply problematic, particularly given that Australia lacks any constitutionally entrenched protection for individual privacy rights. The Australian judiciary accordingly do not have the tools to protect the human rights of Australian citizens from encroachment by the legislature in the same way that EU and US courts have been able to limit the overly-broad collection of metadata. In the Australian legal system, it is the representative parliament that is the primary safeguard of the rights of Australians.

In the remainder of this paper, we seek to understand in more detail how the legislation was passed, and how public interest concerns were addressed during this time. To do so, we look particularly at reports in mainstream media outlets, through which we examine reports of political compromises that were required to secure bipartisan support of the final legislation. The analysis below finds that during the legislative process, the human rights concerns raised by a small group of dissenting voices were not well amplified in the mainstream media. Unlike the much more concentrated complaints of other groups, these concerns were never well addressed by legislators. At least in this case, we show that the legislative process is not well suited to ventilating human rights concerns. This analysis suggests that if human rights of Australians are to be more effectively protected, the judiciary should be empowered to review legislation through constitutionally entrenched rights.

In this part, we review how the act was discussed in the mainstream media from the time it was mooted to the time it was finally passed. We present a qualitative analysis of 1,689 news articles and opinion pieces published in Australian mainstream media outlets and high profile online sources over the period from 1 August 2014 to the passage of the Act on 26 March 2015. Articles were collated through the Factiva news index, searching on the term 'data retention' or 'metadata', for all Australian sources, with duplicates removed. We then inductively analysed each of these articles, coding thematically to identify the key actors and examine how these controversies played out in the popular press over the course of the bill's introduction and

passage through federal parliament. We focus in this article on the two key themes dealt with above – necessity: how the scheme was justified in the national media; and proportionality: how the scheme would be tailored to protect individual privacy interests.

The first thing to note about voices that were represented in the mainstream media is that the conversation was dominated, from the outset and across the eight months we examined, by government MPs and representatives from the federal law enforcement and intelligence agencies. There was strongly worded, relatively consistent opposition from civil society groups and a small number of cross-bench senators throughout the period, but even combined, these voices were present at rates far fewer – roughly half – than government voices, and were generally proportionally better represented in the technology and independent press than the larger mainstream outlets. Members of the Labor opposition are represented at similar rates, but they are generally much more reserved in their critiques of the government's proposal. The telecommunications groups, by comparison, are quite muted throughout the entire period. While the industry body Communications Alliance is at times critical about the costs of the scheme for telecommunications providers, it and the larger telecommunications providers it represents declared their general support early in the debate. Only a small number of ISPs - most particularly iiNet - maintained any real public opposition to the scheme.

A. CONTENT AND METADATA

The lack of clarity around the new regime initially galvanised opposition but was eventually a key factor in the act's successful passage. From the point at which the government announced plans to introduce a data retention regime, the definition of what it would cover has been controversial. Over a few days in early August 2014, both the Prime Minister and the Attorney General struggled to articulate what exactly the term 'metadata' meant. Tony Abbott, Prime Minister at the time, told the Nine Television Network that the scheme would include the addresses of websites that Australians visit ('It's not what you're doing on the internet, it's the sites you're visiting, it's not the content, it's the sites [where] you've been'). His office later clarified that this was not, in fact, within the scope of the scheme: 'The government requires a lawful warrant to look at Australians' web-browsing history. This is not metadata, it's content.' (Grubb & Massola, 2014) Later that same day, Attorney-General George Brandis, in a notoriously disastrous interview with Sky News, also struggled to explain metadata. The Senator appeared to confirm that the addresses of the websites that users visit would in fact be captured. Abbott and Brandis were widely ridiculed on mainstream and social media following these blunders. By Friday, then Communications Minister Malcolm Turnbull was much more emphatic – speaking to ABC Radio, he explained that metadata would not include the addresses of websites that users browse. Instead, Minister Turnbull noted, the scheme would only extend to a subscriber's connection information – the IP address allocated to the subscriber by their ISP – and associated information. This distinction, finally, was also confirmed by the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) in a show of unified force.

Turnbull's efforts to limit the damage caused by the fumbled interviews, rapidly deployed across a large range of media, were only partially effective. These few days in August set the stage for a great deal of confusion over the distinctions between 'metadata' and 'content' over the next six months. The massive attention focused on the scheme in its first week gave rise to one of the most persistent demands by commentators: that the government define, with some precision, exactly what would be caught by the scheme. Hundreds of articles in the mainstream press picked up the story over the next two weeks, and strong opinion pieces came out for and against data retention. A small group of journalists from independent and technology publications, and

technology journalists in mainstream outlets, vocally and consistently criticised the lack of detail in the scheme and the confusion about what it would actually cover. The government did not release clarification of what the scheme would cover until an industry discussion paper was leaked in late August 2014 (Grubb, 2014). This discussion paper specifically excluded web browsing history, but set up the complex table of information that was to be retained in a form similar to the one in the final act.

The complexity of the scheme's scope limited the clarity and effectiveness of public debate. This uncertainty was eventually exploited by the government to its advantage. By the time the government introduced the bill into parliament, on 30 October 2014, Minister Turnbull was able to characterise the retention of web browsing history as the key privacy concern. The government was then able to answer, simply and directly, that this was excluded from the scope of the regime in the draft data set specification released on 31 October 2014. Examination of the bill was immediately referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS). This committee was much more likely to support the bill than the PJCHR; the PJCIS is focused on security, not human rights, and is comprised only of parliamentarians from the two major parties and none of the cross-bench senators or the Labor figures who had been critical of the scheme. The government was able to respond to the ongoing concerns about the scheme by implementing the relatively limited recommendations of the PJCIS to, for example, include the dataset within the text of the act (in s 187AA) and add clarifications that the obligations would not require ISPs to collect details about web browsing or on use of services like webmail or instant messaging that they did not directly provide.

B. NECESSITY AND NATIONAL SECURITY JUSTIFICATIONS

While the government's plans to introduce data retention obligations were framed in national security rhetoric from the start, the extent to which the scheme was actually necessary was never particularly well explained. Early in the debate, prior to December 2014, the agencies struggled to respond to questions expressed in the mainstream media about the necessity of the new rules. The scheme was referred to as the 'third tranche' of the government's national security agenda after expanded surveillance powers and new restrictions designed to deal with Australians fighting abroad.

The law enforcement agencies early on provided little detail about their need for the scheme, beyond asserting the importance of access to metadata for dealing with terrorist threats and serious crime. Various representatives from ASIO, the AFP, the Australian Crime Commission pointed to increasing pressures in dealing with data in modern surveillance and the fact that access to metadata was a routine part of their investigative work, but these claims originally did not resonate strongly in the face of sustained pressure to explain the type of data to be collected and the purposes for which it would be used. On the relatively few occasions that they were pressed, representatives of the agencies and the Attorney-General's Department (AGD) were unable to provide specific evidence that current levels of access were inadequate, or that a requirement to obtain a warrants would significantly interfere with their activities. The key question about why warrantless access was required, on either national security justifications or for the broader category of law enforcement activities that the scheme actually permits, went largely unreported by the media.

The debate changed abruptly in December 2014, after the extremely high profile hostage siege in Sydney by a lone gunman (ABC, 2014). In the wake of the siege, Prime Minister Abbott intensified his appeals to national security concerns as a key priority. Abbott was at this time struggling to maintain his grip on the leadership in the face of continuously declining opinion

poll figures. Over this period, Abbott, Brandis, and representatives from ASIO, the AFP, and the AGD began to put together a cohesive narrative about why this next tranche of national security legislation was required as a matter of urgency. These calls reverberated through the national media and built to a crescendo following the attacks on *Charlie Hedbo* workers in Paris in early January 2015, and the arrest of two men on terrorism charges in Sydney, in February 2015. From December through to March, the government also began adding to the national security claims with much more clearly defined narratives about the key role of telecommunications data in the investigation of other serious crimes – including charging a suspect in a prominent murder investigation, arresting suspects involved in a major drug shipment, and investigating child sexual abuse claims.

The effect of the substantial increase in the force of national security rhetoric is striking. Labor, under Bill Shorten's leadership, became largely unable to publicly criticise data retention for fear of appearing weak on national security. The lack of specificity in the government's justifications early on in the debates had allowed Labor some latitude to critique the scheme. When it was first introduced, Shorten firmly opposed a new 'internet tax' that would see 'ordinary Australians [...] treated as if they are criminals' (Shorten, 2014). Labor's ability to voice public criticism was necessarily muted, however, both on the basis of Labor's support for national security and the fact that it had previously supported data retention in 2012.

But from December, the lack of specificity was exploited by the government to secure the act's passage. In the mass media, the government's urgency to take some action on national security issues substituted for the more pointed and complex questions about why, exactly, a warrantless data retention scheme was necessary. A small number of critics in independent and technology news outlets pointed out that the perpetrators of the Sydney and Paris attacks were already known to law enforcement agencies – and therefore could have been adequately surveilled under existing legal arrangements – but these dissenting voices were not amplified in more mainstream outlets.

Meanwhile, when pressed on criticisms of the scope of the proposed regime, government representatives were able to defer to the PJCIS committee, which was tasked with reviewing the bill. In committee, too, the national security rhetoric increased. When the PJCIS hearings continued after the siege, the agencies were able to present a unified front about the importance of access to telecommunications data in investigations. Opposition members sought to press the government to provide greater detail, and expressed considerable frustration that the details were complex and were not at any rate to be finalised before the committee was due to report in late February. Government members of the committee increased the pressure at this stage; Senator Nikolic, former Attorney-General Ruddock, and Committee Chair Tehan MP, in particular, all well-known for advocacy on national security, provided strong defence for the further proposition that the data retention bill was necessary for ensuring access to telecommunications data. The advocates for data retention were emboldened after the siege, and immediately began calling for even more extensive powers in the national media – in the immediate aftermath, Ruddock and the AFP are separately quoted arguing for a five year retention period.

Before the committee had even released its report, the main political opposition to the bill was essentially over. The increasing strength of the government's rhetoric on national security and crime eventually forced the opposition into a corner. On 5 February, Shorten was still willing to call for delay and care in examining the bill, noting that Labor was committed to national security but committing to wait until the PJCIS report was handed down at the end of the

month. Wedged into supporting national security policy, the Australian Labor Party was only able to critique the process, not the substance, of the proposed data retention scheme. Shorten worked over this period to try to defuse the escalating rhetoric, but was ultimately unsuccessful. By 12 February, three weeks before the PJCIS report was due, the Labor opposition caucus had reportedly come to the conclusion that opposing the bill would provide the embattled Prime Minister with an opportunity to attack Labor and potentially revive his doomed leadership. [2] From this point on, it seemed certain that Labor would support the data retention bill, subject to recommendations of the report.

The PJCIS report, released on 27 February 2015, came out in support of the bill with some recommendations, and it was clear at this stage that the bill would have bipartisan support after a set of relatively minor amendments. In essence, the government was able to navigate criticism of the bill and progress it through parliament by focusing the attention of most media outlets on issues that the government was able to adequately resolve – such as the inclusion of the proposed data set within the legislation – and by using media coverage of the Sydney siege and the Paris attacks to fuel concern about national security. In doing so, more fundamental human rights criticisms about the act were essentially sidestepped.

C. COMPLEXITY AND UNCERTAINTY

Australia's data retention act poses a clear threat to individual privacy in a way that is not clearly justified under international law. While criticisms about the necessity and proportionality of the act were raised by a range of different actors during its passage, the government did not ultimately need to prove its assertion that the act complied with human rights standards. We suggest that a large part of the reason for this is that the vagueness and complexity of the scheme meant that it was not well understood in the mainstream media. This in turn enabled the government to secure support on the broad justifications without needing to justify the details.

Ultimately, neither the necessity of data retention, nor the specific privacy protections to ensure the scheme was a proportionate measure, were dealt with in any detail in the mainstream press. Its necessity was effectively asserted, in general terms, by terror attacks in Sydney in December 2014 and in Paris in January 2015. The intense national security rhetoric deployed over this period by the government and by the agencies on the importance of telecommunications data in investigations stood in for any detailed explanation of the necessity of the particular measures proposed in the bill. Meanwhile, when pressed on the safeguards for privacy, the government was able to delay and defer responses – the detail about what content would be caught and what agencies would have access was only provided in draft form, and the task of ensuring that the act was proportionate was delegated to the Parliamentary Joint Committee on Intelligence, the executive judgment of the Minister, and a system of review by parliament.

When opposition was united around particular, easily understandable issues, the government was forced to make some concessions. Most particularly, very late in the process, the government introduced a specific secret warrant scheme for access to journalists' metadata. Some critics, including the major journalists' union, had been warning for months that the scheme would better empower law enforcement agencies to track down journalists' sources without a warrant. It was only after bipartisan support for the bill had been announced that this concern exploded in the mainstream media, in a storm that threatened to scuttle the bill. This empowered Labor to demand changes, and the government responded with a warrant scheme that applied only to journalists' metadata. While not necessarily satisfactory to media interests, this was sufficient to again secure bipartisan support. The other concerns raised about the bill

were not as well targeted, and the government was largely able to ignore or defer the issues. For example, following the journalists, lawyers' groups unsuccessfully sought exceptions to protect their clients' legal privilege, but these concerns came too late in the process. Similarly, telecommunications providers still sought clarity on costs, but the government was able to delay a decision until after the act was passed.

The most concerning issue with the final act, from the perspective of proportionality, is that the extents of the scheme are vague and subject to ministerial discretion. Both the types of data to be collected and the agencies that are permitted to access this data without any judicial oversight are left to be determined by subordinate legislation. These concerns, however, were never well articulated in the national debate. They were repeatedly raised by a set of clear dissenting voices in independent and technology media outlets, but they were not strongly amplified in mainstream sources. Many legislative details were missing for much of the debate, and when finally presented by the government, were complicated and difficult to understand. This complexity was reflected in much of the mainstream media coverage, which tended - perhaps understandably - to gloss over significant details and, in some cases, progressed on incorrect assumptions about the operation of the scheme. While there were dissenting voices present throughout the debate, it appears from our analysis that the government was ultimately able to exploit the lack of clarity in its own legislation in its favour. The PJCHR's recommendations were, in the end, safely rejected by the government with no real political fallout.

CONCLUSION

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act* was passed by the Australian government in April 2015, and is due to be reviewed by the PJCIS sometime in 2019 (s 187N). However, absent a high-profile court case or renewed vigour in the public debate, it is unlikely that a review will change much about Australia's current data retention scheme. Our analysis of the mainstream media over the course of the passage of the act highlights significant shortcomings in the legislative process. In Australia, where the legislature is primarily responsible for defining (and by implication, protecting) the rights of individuals, we have shown that human rights concerns about mass data retention were poorly ventilated in major policy *fora*. Ultimately, the government was able to pass the legislation with very little interrogation of its claims that data retention is necessary to maintain national security. We suggest that this is particularly concerning in a system without a constitutional bill of rights that is enforceable by an independent judiciary.

In Europe, similar data retention schemes have been found disproportionate to the objective of fighting serious crime, even where that objective was deemed to be a legitimate objective of general interest. Factors that compelled the ECJ to hold that a wide-ranging metadata retention obligation was disproportionate included that the obligation impacted all citizens using electronic communications services regardless of involvement in criminal activity and that there was no requirement that law enforcement agencies obtain a warrant or seek prior review from a court or independent administrative body before accessing a person's metadata. In Australia, similar shortcomings with the government's data retention regime did not have any real impact on the success of the act's passage through parliament. Unlike in other jurisdictions, there is little prospect that these concerns can be raised in any challenge to the validity of the act.

The government asserted, following terror attacks in Sydney in December 2014 and Paris in

January 2015, that extensive data retention was necessary to protect national security. This assertion was not effectively questioned by the Australian mainstream press. But even if data retention is accepted as a necessary intrusion to maintain national security, the government has not included protections to make it a proportionate measure. In this article we have raised concerns about deficiencies in the act, including that the language of the act remains vague; the scope for ministerial discretion about what metadata must be retained and which agencies may access metadata is significant; and there is no judicial oversight before agencies may access Australians' private information.

REFERENCES

Abbott, T. (2015, February 12). Questions Without Notice. Retrieved May 12, 2016, from http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansardr%2Fcb768683-f6bc-44e8-8348-c6bd1dba5e12%2F0114%22

Attorney-General's Department. (2015) Telecommunications (Interception And Access) Act 1979 Annual Report 2014–15, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Telecommunications-Interception-and-Access-Act-1979-Annual-Report-14-15.pdf

Australian Broadcasting Corporation (ABC) (2014, December 16) Sydney siege: Two hostages and gunman dead after heavily armed police storm Lindt cafe in Martin Place. *ABC*. Retrieved from http://www.abc.net.au/news/2014-12-16/sydney-siege-gunman-two-hostages-dead/5969162

Brandis, G. (2015, January 12). One more anti-terror tool. *The Australian*. Retrieved from http://www.theaustralian.com.au/opinion/one-more-antiterror-tool/news-story/b9f48192069443268dec2dfcb04870c5

Brown, I., Halperin, M. H., Hayes, B., Scott, B., & Vermeulen, M. (2015). Towards Multilateral Standards for Surveillance Reform. *Oxford Internet Institute Discussion Paper*. Retrieved from http://papers.ssrn.com/abstract=2551164

Commonwealth of Australia (2015), *Martin Place Siege: Joint Commonwealth-New South Wales review*, Canberra, January 2015.

Crowe, D. (2014, August 6). Tough terror laws target jihadis. *The Australian*. Retrieved from http://at.theaustralian.com.au/link/b7eb7c0de853829d9a475d0ec62f6154?domain=theaustralian.com.au

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, No. C-293/12 and C-594/12 (Grand Chamber, European Court of Justice April 8, 2014). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1

Donohue, L. K. (2014). Bulk Metadata Collection: Statutory and Constitutional Considerations. *Harvard Journal of Law & Public Policy*, *37*(3), 757.

Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015.

European Communities (2000) Charter of Fundamental Rights of the European Union.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Henry Holt.

Grubb, B. (2014, August 27). Secret data retention discussion paper leaked. Retrieved June 15, 2016, from http://www.smh.com.au/digital-life/digital-life-news/secret-data-retention-discussion-paper-leaked-20140827-108yyh.html

Grubb, B., & Massola, J. (2014, August 16). What is "metadata" and should you worry if yours is

stored by law? *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/digital-life/digital-life-news/what-is-metadata-and-should-you-worry-if-yours-is-stored-by-law-20140806-100zae.html

Guy, G. (2016) 'Requests for Access to Telecommunications Metadata under 176A of the TIA', Right to Know, https://www.righttoknow.org.au/request/requests_for_access_to_telecommu

Legal and Constitutional Affairs References Committee. (2015, February 2). Comprehensive revision of the Telecommunications (Interception and Access) Act 1979. Retrieved May 12, 2016, from http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Fcommsen%2F5041f7c9-7d50-4b66-85ef-9796e47cb806%2F0008%22

Murphy, K. (2014, August 12). Data retention: Liberal backbencher calls for metadata warrant requirement. *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/aug/12/data-retention-liberal-backbencher-calls-for-metadata-warrant-requirement

Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance. (2014, May). Retrieved June 18, 2016, from https://necessaryandproportionate.org/principles

Obama, B. (2014, January 17). Presidential Policy Directive 28. Retrieved June 18, 2016, from https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

Parliamentary Joint Committee on Human Rights. (2014, November 14). Fifteenth Report of the 44th Parliament. Retrieved June 15, 2016, from http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Completed_inquiries/2014/Fifteenth_Report_of_the_44th_Parliament

Parliamentary Joint Committee on Human Rights. (2015, March 18). Twentieth Report of the 44th Parliament. Retrieved June 19, 2016, from http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Completed_inquiries/2015/Twentieth_Report_of_the_44th_Parliament

Parliamentary Joint Committee on Intelligence and Security. (2015, January 30). Retrieved May 12, 2016, from http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F643492e1-2923-4bc9-9afa-09fd87d7f065%2F0006;query=Id%3A%22committees%2Fcommjnt%2F643492e1-2923-4bc9-9afa-09fd87d7f065%2F0000%22

Review Group on Intelligence and Communications Technologies. (2013). *Liberty and Security in a Changing World*. Retrieved from https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Taylor, J. (2016, January 18). Over 60 agencies apply to snoop into your metadata. *Crikey*. Retrieved from https://www.crikey.com.au/2016/01/18/over-60-agencies-apply-to-snoop-into-your-metadata/

Tele2 Sverige AB v Post-och telestyrelsen (C203/15) and Secretary of State for the Home

Department v Watson, Brice and Lewis (C-698/15) (joined cases) (Grand Chamber, European Court of Justice, December 21, 2016). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=828733.

Shorten, B. (2014, August 6). Doorstop: Canberra. Retrieved June 15, 2016, from http://www.billshorten.com.au/doorstop-canberra-10

United Nations. (1948) Universal Declaration of Human Rights.

United Nations. (1966). International Covenant on Civil and Political Rights.

United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, & Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights. (2013, June 21). Joint Declaration on surveillance programs and their impact on freedom of expression. Retrieved June 18, 2016, from http://www.oas.org/en/iachr/expression/showarticle.asp?artID=926&lID=1

FOOTNOTES

1. In a judgment handed down on 21 December 2016 in the joined cases of Tele2 Sverige AB v Post-och telestyrelsen (C203/15) and Secretary of State for the Home Department v Watson, Brice and Lewis (C-698/15) (Tele2 Sverige), the Grand Chamber of the European Court of Justice (ECJ) confirmed that the Digital Rights Ireland decision, together with article 15(1) of Directive 2002/58/EC as amended by Directive 2009/136/EC and read in light of articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union, precluded "national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication" (Tele2 Sverige [112], [134]). The ECJ further held that national legislation governing the protection and security of traffic and location data, and the access of that data by competent national authorities, would be precluded where it was not restricted solely to fighting serious crime, where access was not subject to prior review by a court or an independent administrative authority, and where there was no requirement that the data should be retained within the European Union ([125], [134]). The Tele2 Sverige decision arose from two separate cases concerning the scope of national data retention legislation in Sweden (Tele2 Sverige AB v Post- och telestyrelsen, Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) 29 April 2015) and England (The Queen v Secretary of State for the Home Department [2015] EWHC 2092). Both cases were referred to the ECJ for clarification on the impact of Digital Rights Ireland as to general data retention legislation at a national level.

2. Abbott was eventually deposed by Malcolm Turnbull in September 2015: http://www.abc.net.au/news/2015-09-14/malcolm-turnbull-beats-tony-abbott-in-liberal-leadership-ballot/6774546.