The limits of (digital) constitutionalism:

Exploring the privacy-security (im)balance in Australia

1. Dr Monique Mann

   School of Justice, Faculty of Law

   Queensland University of Technology

   2 George St, Brisbane, 4000, QLD

   Email: m6.mann@qut.edu.au

2. Dr Angela Daly

   School of Law, Faculty of Law

   Queensland University of Technology

3. Mr Michael Wilson

   School of Justice, Faculty of Law

   Queensland University of Technology

4. Associate Professor Nicholas Suzor

   School of Law, Faculty of Law

   Queensland University of Technology

Abstract

This article explores the challenges of digital constitutionalism in practice through a case study examining how concepts of privacy and security have been framed and contested in Australian cyber security and telecommunications policy-making over the last decade. The Australian Government has formally committed to 'Internet freedom' norms, including privacy, through membership of the Freedom Online Coalition. Importantly, however, this commitment is non-binding and designed primarily to guide the development of policy by legislators and the executive government. Through this analysis, we seek to understand if, and how, principles of digital constitutionalism have been incorporated at the national level. Our analysis suggests a fundamental challenge for the project of digital constitutionalism in developing and implementing principles that have practical or legally binding impact on domestic telecommunications and cyber security policy. Australia is the only major Western liberal democracy without constitutional human rights or a legislated bill of rights at the federal level; this means that the task of 'balancing' what are conceived as competing rights is left only to the legislature. Our analysis shows that despite high-level commitments to privacy as per the Freedom of Online Coalition, individual rights are routinely discounted against collective rights to security. We conclude by arguing that, at least in Australia, the domestic conditions limit the practical application and enforcement of digital constitutionalism's norms.

Key words: Privacy, security, securitisation, cyber security, online surveillance, metadata retention, human rights, digital constitutionalism

Introduction

This paper examines how formal commitments to digital constitutionalism and protecting the human rights of individuals in domestic policy-making are reflected in Australian telecommunications and cyber security policy. As a case study, we examine how conceptions of privacy and security are constructed in Australian policymaking discourses. We focus specifically on Australia due the unique domestic context. Despite Australia's recent commitment to online privacy as per the Freedom of Online Coalition, there is an absence of constitutional protections of human rights and corresponding enforcement mechanisms – a scenario which may be replicated in a United Kingdom 'Brexited' from the European Union and Council of Europe human rights protections. Further, as a member of the Five-Eyes partnership, Australia has been heavily involved in global surveillance practices.

Both the privacy and security interests of individuals are often promoted via 'digital constitutionalism', that is the 'constellation of initiatives that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet' (Gill et al., 2015: 2). Reflecting multistakeholder Internet governance processes (Waz and Weiser, 2013), these initiatives have emanated from international organisations, national governments, technology companies and civil society groups. Traditional, pre-digital forms of constitutionalism have generally sought to address exercises of power by the nation-state (Waldron, 2012), but more recent endeavours have sought to address the practices of private companies (often large and transnational entities) that provide critical Internet services, platforms and infrastructure (Gill et al., 2015; Suzor, 2010). In their analysis of digital constitutionalism policy documents, Gill et al. (2015) found that privacy rights were

among the three most prominent rights in these documents, with the right to personal security and dignity appearing less often, but still present in eight of the documents analysed.

However, apart from the Brazilian *Marco Civil*[1], the digital constitutionalism project so far has generally resulted in aspirational targets for nation-states, international organisations and private Internet actors, rather than enforceable rights in domestic legal systems (Gill et al., 2015). The *Marco Civil* is unique given its status as binding legislation from a nation-state, albeit one that 'fleshes out rights that already exist in Brazil (albeit in a latent or vague form), rather than creating entirely new rights' (Mendeiros and Bygrave, 2015: 121). Aside from the *Marco Civil*, the lack of domestic legal protection and corresponding enforcement mechanisms is a major challenge for the digital constitutionalism project. Digital constitutionalist declarations, like many international human rights instruments, can be difficult to enforce in a practical sense at the nation state level.

Similar to these international human rights agreements (von Stein, 2016), and via an analysis of Australian policymaking processes, we argue the domestic situation is central to determining the extent to which law and policy reflect digital constitutionalist norms. Where rights are not supported by mechanisms for judicial enforcement, there is a risk that legislative processes may fail to adequately protect

[1] A Magna Carta for Philippine Internet Freedom has been put before the Parliament of the Philippines but, at the time of writing, has not been signed into law (Robie and Abcede, 2015). The Italian Declaration of Internet Rights, is 'an exclusively political document with no legal binding value' (Pollicino and Bassini, 2015). The Nigerian Parliament has been considering legislation to enact a 'Nigerian Digital Rights and Freedoms Bill' (Yilma, 2017).

individuals' rights. This can be seen as a limitation of the digital constitutionalism project in addition to the other limitations identified by Yilma (2017), namely: fragmentation; disjointed goals; a lack of feasibility; the Western perspective that many if not most of the digital constitutionalism initiative adopt; and the lack of engagement with the digital divide between developed and developing countries, and internally within countries.

In order to better understand these policymaking processes and compromises we collected a sample of documents about the development of Australian telecommunications and cyber security policy across the previous decade (2007-17). We analysed policies developed by the Commonwealth government and its agencies and inquiries conducted by the Australian Parliament that were published between 2004 and 2016. These documents are moulded by the political process and are representations of policy development and governance (Barnard-Wills, 2013). Using narrative policy analysis we traced policy development through time to identify the rhetoric used to justify government decision-making (Van Eeten, 2008: 251; Roe, 1994). We examined how the notions of privacy and security as individual or collective rights are discursively constructed, and whether they were framed as competing or complementary.

Digital Constitutionalism in Australia

Australia has formally adopted some principles of digital constitutionalism, most prominently by joining the Freedom Online Coalition (FOC) in 2015, 'a group of governments who have committed to work together to support Internet freedom and protect fundamental human right – free expression, association, assembly, and privacy

online – worldwide' (Freedom Online Coalition, n.d.). FOC members commit to the shared goals and values of the Tallinn Agenda, which envisages 'respect for human rights and fundamental freedoms and security online [being] complementary concepts' (Freedom Online Coalition, 2014: 1). It is important to note, however, that despite these high-level commitments to digital rights, no enforcement mechanisms have been implemented in order to ensure compliance.

Despite these high level commitments to digital constitutionalism, Australia is unique as the only Western-style liberal democracy that does not have a comprehensive set of human rights in its Constitution (like the US) or a legislated Bill of Rights (like neighbouring New Zealand) at the federal level. Of the few rights that do receive constitutional protection in Australia, privacy and individual security are not among them, and free expression receives only limited protection via the implied right to political communication (Nicholls, 2012; Pearson, 2012). At the state and territory level in Australia, the Australian Capital Territory (ACT) and the State of Victoria both have human rights legislation which introduces individual rights including privacy and personal security.[2] However the enforcement mechanisms for these bills of rights are weak: courts cannot invalidate laws for a lack of compliance with the enumerated rights (Williams, 2006). The lack of enforceable protections leaves many groups vulnerable to human rights violations and without any means of redress (Otto and Wiseman, 2001). There are various areas of current concern where the Australian government may be violating international human rights standards,

[2] At the time of writing a legislated Bill of Rights is under consideration in the state of Queensland (Williams and Reynolds, 2016).

particularly in regard to refugees (Saul, 2012; Henderson, 2014),[3] and Indigenous/ First Nations peoples (Bielefield and Altman, 2015).

In recent years, the Australian government's surveillance of communications has been a key area of concern for the protection of human rights, specifically privacy. Australia has been heavily involved in global surveillance practices as one of the Five Eyes partners (along with the US, UK, New Zealand and Canada) exposed in the Snowden revelations (Ruby, 2015). While Australians enjoy some personal data protection in domestic law via the *Privacy Act 1988* (Cth),[4] this legislation contains considerable exemptions for law enforcement agencies, including complete exemption for federal law enforcement and intelligence agencies (Greenleaf, 2001; Molnar and Parsons, 2016; Mann and Smith, 2017). These exemptions have the practical effect of trading off individual rights for community interests in security (Bronitt and Stellios, 2005). The *Privacy Act* also did not prevent data retention legislation (based on the now-invalidated EU Data Retention Directive) being introduced (Daly, 2016). This situation can be understood as an example of 'counter-law' (Ericson, 2007) legally facilitating blanket surveillance of the Australian population.

Through these examples it is evident that Australia's commitment to protect individual privacy, as part of the Freedom Online Coalition, is not supported by any

[3] In February 2017, a submission was made to the International Criminal Court requesting that the ICC investigate possible crimes against humanity as regards Australia's offshore asylum seeker detention regime (Doherty, 2017).
[4] This realizes Australia's obligations under the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

real legal enforcement mechanism. Without a constitutional guarantee, the task of protecting privacy in Australia falls to the legislative and executive branches of government. The judicial branch, which has proved important to upholding privacy interests in other Western democracies, has only a limited role in protecting human rights in Australia. Aside from the apparently contradictory results where individuals within a liberal democracy have access few effective options to uphold and enforce their rights via judicial mechanisms, Australia may also serve as a warning tale to those in the United Kingdom faced with a Brexit situation possibly involving the disapplication of EU law (and the Charter of Fundamental Rights) and an exit from the European Convention on Human Rights (Daly and Thomas, 2017).

The Privacy and Security (Im)Balance?

The balancing of security and civil rights is a 'crucial legal conflict in the information society' (Durante, 2013: 437). This regulatory 'conundrum' (Bagby, 2012: 1454) has a 'rhetorical ring that fits the political agenda of extended law enforcement competences' (Hildebrandt, 2013: 372). It has been argued that this conflict 'explains much in the law enforcement, internal private security, counter-terrorism, cyber-security and critical infrastructure protection debates' (Bagby, 2012: 1454). However, the privacy-security relationship may not be a 'balance' but rather a 'trade-off' with the image of the scale used to justify the sacrifice of liberties (Hildebrandt, 2013). Policies are rationalised with the promise of security, but at the expense of other rights and freedoms, including privacy.

Trading privacy for security is often used to support the introduction of new powers and programs of surveillance (de Zwartz et al., 2014; Lachmayer and Witzleb, 2014) and is underpinned by an assumption that security can be achieved through pre-

emptive intelligence-based identification of previously unknown threats (Zedner, 2009; McCulloch and Pickering, 2010). It has been argued that the requirement to pre-emptively identify threats provides 'ready rhetorical support' for the ongoing expansion of surveillance, particularly in online contexts (Barnard-Wills, 2013: 173, 180). Claims to collective security will always outweigh individual rights that are perpetually 'traded off' (Bronitt and Stellios, 2006). Indeed, 'giving up a measure of privacy to gain a measure of security sounds reasonable to many people' (Hildebrandt, 2013: 372).

This privacy-security trade-off can be linked back to broader legal discussions of rights. Human rights are said to be incommensurable, but real-life scenarios of conflicting rights require some sort of balance to be struck between them, especially in the judicial context (McCrudden, 2008). However, there is limited guidance about how to attain a suitable balance between rights, or indeed, what this would represent in practice (Bagby, 2012). Cost-benefit analyses imply precision and quantifiable methods of weighting interests (Hildebrandt, 2013). Yet human rights do not lend themselves easily to quantification. For this reason it has been argued that this 'calculus is highly complex' and simultaneously 'overly simplistic' (Bagby, 2012: 1453, 1454). Some constitutional courts have adopted 'proportionality' analyses to resolve conflicts of fundamental rights (i.e. whether the restriction on a right furthers a legitimate aim in a rational and proportional fashion) (McCrudden, 2008). Yet these analyses have been criticised for constituting a misguided quest for objectivity and precision, where instead courts should be focusing on the moral issues underpinning the conflict of rights (Tsakyrakis, 2009) or engaging in more principled and pragmatic decision-making (De Schutter and Tulkens, 2008). In the absence of 'determinist or

formulaic balancing methodology,' political pressures may be the most significant influence in determining what the outcome of the balancing exercise means for policy (Bagby, 2012: 1453).

The concepts of 'privacy' and 'security' have multiple meanings across a range of contexts. It has been argued that privacy should not be reduced to an individual interest, as it is central to the formation of relationships and the healthy functioning of democracy; a collective right (Bennett, 2011; Regan, 2002; Introna, 1997). Hildebrandt (2013: 364) highlights that privacy may be considered as a social construct 'determined by cultural norms and values'; privacy is contextually dependent. There have also been critiques of the notion of 'security' and particularly 'collective security' or 'national security' as it 'fails to address the conceptual and practical variations that distinguish between the essentially dissimilar interests of states and interests of individuals' (Biletzki, 2013: 399). There are numerous uses and meanings of 'security', and the relationship between security and other rights is complex. Increasing attention is being paid to the notion of 'personal security' that relates to the protection of individual human rights such as privacy (Biletzki, 2013).

We adopt the theoretical lens of securitisation which enables examination of the construction of threats to security, and the development of corresponding technologies of governance. Once an issue is 'securitised', it enables action to be taken against the threat: 'the securitising formula is that such threats require exceptional measures and/or emergency action to deal with them' (Buzan, 1997: 14). The state requires the existence of threats to attest to its legitimacy to govern (see generally Garland, 2002).

It has been argued that 'what becomes defined as a privacy or security "problem"' (and what is excluded from this) is a political process, conducted at least in part through policy texts and documents' (Barnard-Wills, 2013: 170). Barnard-Wills (2013) analysed policy documents from a select group of EU member states and the US. The main findings of this study were that national security consistently provided rhetorical support for the pre-emptive identification of threats to security and increased surveillance. However, it was also found that the EU policy documents advocated a position where 'privacy' and 'security' were not in direct opposition. The point of divergence with Australia however is the absence of comprehensive constitutional or enforceable human rights protections at the federal level. Therefore, in this paper we seek to understand how concepts of, and conflicts between, digital privacy and security are constructed in Australian policy-making over the last decade and how this interaction may influence the realisation of Australia's recent commitments to FOC norms and the wider digital constitutionalism project.

Results and Discussion

In our analysis of the policy documents, five main themes emerge as regards to the relationship between privacy and security in Australian telecommunications and cyber security policy.

1. *Constructing Threats to Security*

In a study of the concepts of privacy and security in European policy documents it was found that the notion of national security has expanded **'**to include *information* security, often under the rhetoric of cyber security, critical infrastructure or cybercrime' (emphasis in original) (Barnard-Wills, 2013: 174). These new 'cyber

threats' – which emerged as a result of new technology and widespread dependence upon it - centre and construct the protection of critical infrastructure as 'an issue of economic competitiveness and prosperity as well as security' (Barnard-Wills, 2013: 174). Indeed, within the sample of policy documents, narratives of securitisation presented risks to both individual and collective security, and the broader economic prosperity of the Australian state. These encompassed threats to national security, critical infrastructure, and the community. An absence of social control and regulatory measures in cyberspace was emphasised; the internet, and more so online anonymity, is framed as a fundamental security risk. For example:

> 'As the quantity and value of electronic information has increased so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying out their activities.' (Attorney-General's Department, 2009: 2).

At the same time, however, there was explicit acknowledgement that the language used to describe threats informs the response:

> 'The broad adoption of the term [cyber attack] has seen it often used in a sensationalist way - similar to 'cyber war', 'cyber terrorism' and 'cyber weapons' - with the term 'attack' generating an emotive response and a disproportionate sense of threat... and undermines the development and application of proportionate nation state responses.' (Australian Cyber Security Centre, 2016: 5).

This highlights how the construction of threats translates into legal and policy responses; threats to national security operate to justify new solutions in policy and practice. These include new powers of surveillance and the introduction of a

mandatory data retention regime (e.g. House of Representatives Standing Committee on Communications, 2010: 2; Parliamentary Joint Committee on Intelligence and Security [PCJIS], 2015: 3)

2. Privacy and Security as Competing Rights

The main rhetorical device that is used to justify the introduction of new laws and policies is balancing privacy and security. This frames the relationship between privacy and security as a compromise or 'zero-sum game' (Bagby, 2012; Hildebrandt, 2013). In order to defend and protect against threats the policy documents show a need to sacrifice individual rights:

> 'Confronting and managing these risks must be balanced against the civil liberties of Australians, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy.' (Attorney-General's Department, 2009: 4).

Further, it was evident in the policy documents that the state considers its own role as sole arbitrator of which normative rights and values can be 'trade-off', which also raises questions about the function of other organs of the state, and appropriate checks and balances (PJCIS, 2013: 190).

This eschews a range of practical considerations and questions of impact. For example, it is implicitly assumed that new powers of surveillance will lead to increased security. These arguments are presented without empirical evidence and operate to 'achieve a largely illusionary public sense of security' (Hildebrandt, 2013: 375). This is related to broader debates that relate to evidence-based policy and the

political capital provided by crime and security as areas of governance (Hildebrandt 2013: 375; Garland, 2002).

3. Privacy and Security as Complementary Rights

At other times the policy documents presented an alternate conception of the relationship between privacy and security as interdependent, mutually reinforcing and complementary. There was recognition that some degree of privacy is necessary for individual liberty and security, particularly in relation to the threat of cybercrime. It was acknowledged that the protection of personal information is necessary to guard against threats such as identity theft, fraud, and other forms of cybercrime:

> 'The Committee agrees that privacy protections are integral to mitigating the risks of cyber crime. Where personal information is well protected, the scope for identity theft and fraud is reduced.' (House of Representatives Standing Committee on Communications, 2010: 202).

These threats are constructed as an outsider criminal threat or as a consequence of new technology, rather than a result of state intrusion and surveillance. A study of European policy documents also found threats were constructed as 'portrayed as coming from information technology' rather than from the state (Barnard-Wills, 2013: 176). Technological determinism was also evident in Australian policy documents:

> 'Vast amount of personal information are increasingly being transmitted over the Internet and stored on digital devices… this growing amount of digitised personal information places end users at a higher risk of identity theft and fraud, and [it has been] argued that ensuring the privacy of end users' personal information is

central to the prevention of cybercrime' (House of Representatives Standing Committee on Communications, 2010: 191).

4. Contradictions and Tensions in Policy Rhetoric

In addition to the above rhetorical strategies, the analysis revealed contradictions both within and across policy documents. For example, there was recognition that there is a need to secure information through privacy-enhancing technologies and encryption, but that those same methods create additional risks to security. Certainly it has been argued that these technologies are 'adaptable to complement' both privacy and security, but do not support the 'expectation of privacy itself, nor does any tool adequately impart the condition of achieving security' (Bagby, 2012: 1458). This reveals how the state constructs this as a barrier to accessing information:

> 'The Government supports the use of encryption to protect sensitive personal, commercial and government information. However, encryption presents challenges for Australian law enforcement and security agencies in continuing to access data essential for investigations to keep all Australians safe and secure.' (Australian Government, 2016: 33).

These tensions and contradictions extend to the primary purpose of new law and enhanced surveillance powers. For example, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) stated that the primary objective of data retention legislation is to protect privacy:

> 'The primary objective of the current legislation governing access to communications is to protect the privacy of users of telecommunications' (PJCIS, 2013: 10).

This flawed and contradictory rationalisation as a consequence of conceptual confusion justifies the introduction of new laws, which serve to impinge on individual privacy rather than protect it. It supports the intrusion of state power in cyberspace that ultimately puts 'individual rights, such as privacy, anonymity and freedom of speech, under sharp devaluating pressure' (Taddeo, 2013: 353).

5. *Offsetting the Balance: Necessity, Proportionality and Safeguards*

The resolution of these 'trade offs' and contradictions occurred through invoking strategies or devices to 'offset' 'losses' in privacy. These arguments centred on the necessity and the proportionality of new powers and surveillance programs. Hildebrandt (2013: 358) has outlined a test in which powers of intrusion may be necessary, arguing this 'requires a legitimate aim, necessity and proportionality, specificity, foreseeability and safeguards.' Her analysis extends beyond law and also considers 'purposiveness, justice and legal certainty of law in a constitutional democracy' (Hildebrandt, 2013: 359). Yet in the policy documents analysed, it was neither explained how 'necessity' is measured nor what measures may be 'proportionate' to. While necessity and proportionality were recurring rhetorical devices used to justify certain cyber security policy positions, they were just that: rhetoric without substance. For example:

> 'The evidence received by the committee emphasised that the right to access telecommunications information should only be exercised when both proportionate and appropriate' (Legal and Constitutional Affairs References Committee, 2012: 12-13).

Another device that is used to 'offset' the 'trade-off' between privacy and security is the promise of the introduction of new and strengthened accountability structures and safeguards. It has been argued, 'whenever we increase the employment of security measures that violate our liberties, this warrants extra safeguards to regain the balance' (Hildebrant, 2013: 357). This cements the image of the scale with further 'balancing' via the introduction of new and improved checks and balances as an interesting parallel rhetorical device:

> 'A balance must be struck between appropriate checks and balances, and the operational flexibility required to deliver effective law enforcement and protection against national security threats' (PJC IS, 2013: 47).

Yet, in practice such increased accountability structures and safeguards have either not been implemented, have been under-funded, or there have been attempt to circumvent those that have been implemented. For example, in the data retention scheme, a limited number of Australian government agencies were given warrantless access to retained data, but it emerged that agencies without such access were circumventing this safeguard by funnelling data requests through one of the authorised bodies, the Australian Federal Police, seemingly encouraged to do so by the Attorney-General's Department (Sveen, 2016).

Conclusion

Our analysis of Australian cyber security and telecommunications policy documents over the last decade demonstrates various aspects of the privacy-security relationship domestically, with implications for Australia's commitment to, and implementation of, digital constitutionalism norms.

We found that the way in which threats are framed determines the response. Threats are framed in a technologically deterministic way, as coming from external actors and technology itself rather than the state. In order to address these threats, the state requires further powers, itself becoming a (unacknowledged) threat to individuals' rights. In these discussions, the relationship between concepts of privacy and security is confused. At times, privacy 'must' be traded off against security in order to address threats, with the consequence of more invasive powers for the state. However when discussing cybercrime, for instance, there is recognition of the complementary relationship between privacy and security, but again this occurs as a result of external criminal threats and the narrative positions the state as protector of both rights. This results in little practical difference between the 'competing' and 'complementary' approaches to privacy and security as both of these policy narratives lead to the same role for the state and outcomes for individual privacy. One consequence of this relationship between privacy and security is absurd claims in some cases, such as the purpose of introducing mandatory data retention being to protect individual privacy!

There was a recognition that the rhetoric of 'accountability' was needed to justify intrusions. 'Necessity' and 'proportionality' were recurring rhetorical devices used to justify certain cyber security policy positions, but they were just that: rhetoric without substance. Empirical evidence was generally not adduced to support the state's identification of threats and the necessity and proportionality of privacy-invasive measures to address these threats. Reference is made to accountability measures as a means of offsetting privacy-invasive law and policy but again this was largely rhetorical, and even when accountability measures were introduced,

government practice did not always respect them. Thus, even where the language of digital constitutionalism is used, in the absence of legal enforceability, the rhetoric is largely meaningless.

Our analysis shows that the development of Australian telecommunications and cyber security policy over the last decade has been inconsistent with digital constitutionalist norms of privacy and security. The historical trajectory of this policy has not been consistent with FOC norms. Even subsequent to Australia joining the FOC and making a public commitment to these norms in 2015, Australia continues to develop policies which are not compliant with these norms, notably the introduction of mandatory data retention and its ongoing implementation. In fact, since Australia has joined the FOC, the level of Internet freedom in the country, as measured by Freedom House (2015), has actually declined. Yet Australia is not alone: other FOC members, including the UK and US, have also fallen short of implementing FOC norms (Carlson, 2014; York, 2014), pointing to a discrepancy between what FOC members have committed to do and what they do in practice (Morgan 2016).

The policy discourse around the conflict between security and privacy interests in Australia illuminates a fundamental challenge for the digital constitutionalism project. The non-binding, aspirational nature of the major digital rights declarations is problematic. Our case study shows how digital constitutionalist rights can be overridden by the internal activities of nation-states, especially in response to circumstances and technologies framed by the nation-state as threats. It should be noted that individuals in Australia are in a weaker positions compared to their counterparts in other non-compliant FOC countries such as the US and UK,

where for the moment, ‘pre-digital’ constitutional and human rights protections permit a means of challenging this non-compliance with privacy and security rights in domestic and regional courts. Thus, to be effective, digital constitutionalism also requires certain ‘background’ constitutional arrangements to be present if individuals are to be fully able to realise these rights – arrangements which are absent in Australia’s case.

References

Australian Cyber Security Centre (2016) Threat Report. Available at: *https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf*

Australian Government (2016) Australia's Cyber Security Strategy. *Available at: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf*

Attorney-General's Department, Australian Government (2009) Cyber Security Strategy. Canberra: Attorney-General's Department. Available at: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20- %20for%20website.pdf

Bagby J W (2012) Balancing the public policy drivers in the tension between privacy and security' In K J Knapp (ed.) *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*. Hershey, Pennsylvania: Information Science Reference, 164-183.

Barnard-Wills D (2013) Security, privacy and surveillance in European policy documents. *International Data Privacy Law* 3(3): 170-180.

Bennett C (2011) In defence of privacy: The concept and the regime. *Surveillance & Society* 8(4): 485-496.

Bielefeld S and Altman J (2015) Australia's First Peoples – Still struggling for protection against racial discrimination. In: *Perspectives on the Racial Discrimination Act: Papers from the 40 years of the Racial Discrimination Act 1975 (Cth) Conference*, Sydney, Australia, 19-20 February 2015, pp. 196-206. Sydney: Australian Human Rights Commission..

Biletzki A. (2013) Online security: What's in a name? *Philosophy and Technology* 26*:* 397-410.

Bronitt S and Stellios J (2005) Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects. *Telecommunications Policy* 29(11): 875-888.

Bronitt S and Stellios J (2006) Regulating telecommunications interception and access in the twenty-first century: Technological evolution or legal revolution? *Prometheus* 24(4): 413-428.

Buzan B (1997) Rethinking security after the Cold War. *Cooperation and Conflict* 32(1): 5-28.

Carlson K (2014) EFF Joins Coalition Calling on FOC Member States to Live up to Their Stated Commitment. In *EFF Deeplinks Blog.* Available at: https://www.eff.org/deeplinks/2014/04/eff-calls-members-freedom-online-coalition-assess-their-stated-commitments

Daly A (2016) Digital rights in Australia's Asian century: A good neighbour? In *The Good Life in Asia's Digital 21st Century*. Hong Kong: Digital Asia Hub, 128-136.

Daly A and Thomas J (2017) Australian Internet Policy. *Internet Policy Review* 6(1).

de Zwart M, Humphreys S and van Dissel B (2014) Surveillance, big data and democracy: Lessons for Australia from the US and UK. *UNSW Law Journal* 37(2): 713-747.

De Schutter O and Tulkens F (2008) Rights in conflict: The European Court of Human Rights as a pragmatic institution. In E Brems (Ed) *Conflicts Between Fundamental Rights.* Antwerp, Belgium: Intersentia, 169-216.

Doherty B (2017) International Criminal Court told Australia's detention regime could be a crime against humanity. *The Guardian,* 3 February. Available at:

https://www.theguardian.com/australia-news/2017/feb/13/international-criminal-court-told-australias-detention-regime-could-be-a-against-humanity

Durante M (2013) Dealing with legal conflicts in the information society. An informational understanding of balancing competing interests. *Philosophy and Technology* 26: 437-457.

Ericson R V (2007) Security, surveillance and counter-law. *Criminal Justice Matters* 68(1): 6-7.

Freedom House (2015) *Australia. Freedom on the Net 2015 Report*. Freedom House, U.S.A.

Freedom Online Coalition (n.d.) About Us. Available at: https://www.freedomonlinecoalition.com/about/

Freedom Online Coalition (2014) Recommendations for freedom online adopted in Tallinn, Estonia on April 28, 2014 by Ministers of the Freedom Online Coalition. Available at: https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

Garland D (2002) *The Culture of Control*: *Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.

Gill L, Redeker D and Gasser U (2015) Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. Report by Berkman Center Research, Publication No 2015-15.

Greenleaf G (2001) 'Tabula rasa': Ten reasons why Australian privacy law does not exist. *University of New South Wales Law Journal* 24(1): 262-269.

Henderson C (2014) Australia's treatment of asylum seekers: From human rights violations to crimes against humanity. *Journal of International Criminal Justice* 12(5): 1161-1181.

House of Representatives Standing Committee on Communications, Parliament of the Commonwealth of Australia (2010) Hackers, Fraudsters and Botnets: Tacking the Problem of Cyber Crime. Available at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/report/full_report.pdf

Hildebrandt M (2013) Balance or trade-off? Online security technologies and fundamental rights. *Philosophy and Technology* 26: 357-379.

Introna L (1997) Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy* 28(3): 259-275.

Lachmayer K and Witzleb N (2014) The challenge to privacy from ever increasing state surveillance: A comparative perspective. *UNSW Law Journal* 37(2): 748-783.

Legal and Constitutional Affairs References Committee, Parliament of Australia (2015) Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979. Available at: *http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Report*

Mann M and Smith M (2017) Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal* 40(1). Available at: https://eprints.qut.edu.au/102300/

McCrudden C (2008) Human dignity and judicial interpretation of human rights. *European Journal of International Law* 19(4): 655-724.

McCulloch J and Pickering S (2010) Future threat: Pre-crime, state terror, and dystopia in the 21st century. *Criminal Justice Matters* 81(1)*:* 32-33.

Mendeiros F and Bygrave L (2015) Brazil's *Marco Civil da Internet*: Does it live up to the hype? *Computer Law & Security Review* 31(1): 120-130.

Molnar A and Parsons C (2016) Drones and law enforcement in Australia and Canada: Governance through 'privacy' in an era of counter-law? In R Lippert, K Walby, I Warren and D Palmer (Eds.) *Security, Surveillance and Law in Comparative Context*. Kent, United Kingdom: Palgrave, 225-247.

Morgan S (2016) Clarifying goals, revitalizing means: An independent evaluation of the Freedom Online Coalition. Report for Internet Policy Observatory, 5-2016. Available at: http://repository.upenn.edu/internetpolicyobservatory/2

Nicholls N (2012) Right to privacy: Telephone interception and access in Australia. *IEEE Technology and Society Magazine* 31(1): 42-49.

Otto D and Wiseman D (2001) In search of 'effective remedies': Applying the International Covenant on Economic, Social and Cultural Rights in Australia. *Australian Journal of Human Rights* 7(1): 5-46.

Pearson M (2012) The media regulation debate in a democracy lacking a free expression guarantee. *Pacific Journalism Review* 18(2): 89-101.

Pollicino O and Bassini M (2015) An Internet Bill of Rights? Pros and cons of the Italian way. In: LSE Media Policy Project Blog. Available at: http://blogs.lse.ac.uk/mediapolicyproject/2015/08/05/an-internet-bill-of-rights-pros-and-cons-of-the-italian-way/

Parliamentary Joint Committee on Intelligence and Security (2013) Report of the Inquiry into Potential Reforms of Australia's National Security Legislation. Available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm

Parliamentary Joint Committee on Intelligence and Security (2015) Advisory Report on the Telecommunications (interception and Access) Amendment (Data Retention) Bill 2014. Available at: *http://www.aph.gov.au/~/media/02%20Parliamentary%20Business/24%20Committees/244%20Joint%20Committees/PJCIS/DataRetention2014/FinalReport_27February2015.pdf*

Privacy Act (Cth) (1988). Available at: http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

Regan P (2002) Privacy as a common good in the digital world. *Information, Communication & Society* 5(3): 382-405.

Robie D and Abcede D (2015) Cybercrime, criminal libel and the media: From 'e-martial law' to the Magna Carta in the Philippines. *Pacific Journalism Review,* 21(1): 211-229.

Roe, E (1994) *Narrative Policy Analysis: Theory and Practice.* Durham, CT: Duke University Press.

Ruby F (2015) Five eyes over the planet. *Líneasur* 3(9): 34-46.

Saul B (2012) Dark justice: Australia's indefinite detention of refugees on security grounds under international human rights law. *Melbourne Journal of International Law* 13(2): 685-731.

Standing Committee on Communications (2010) Hackers, fraudsters and botnets: Tackling the problem of cyber crime. Available at: http://www.aph.gov.au/parliamentary_Business/Committees/House_of_Representatives_Committees?url=coms/cybercrime/report.htm

Sveen B (2016) Data retention bill: Government departments ask AFP to access metadata after legislation enacted. *ABC News,* 4 October. Available at:

http://www.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648

Suzor N (2010) The role of the rule of law in virtual communities. *Berkeley Technology Law Journal* 25(4): 1817-1886.

Taddeo M (2013) Cyber security and individual rights, striking the right balance. *Philosophy and Technology* 26: 353-356.

Tsakyrakis S (2009) Proportionality: An assault on human rights? *International Journal of Constitutional Law* 7(3): 468-493.

Van Eeten, M (2008) Narrative policy analysis.In F Fischer, G J Miller, and M S Sidney (Eds.) *Handbook of Public Policy Analysis: Theory, Politics, and Methods*, 251-269. Boca Raton, Florida: CRC Press.

von Stein J (2016) Making promises, keeping promises: Democracy, ratification and compliance in international human rights law. *British Journal of Political Science* 46(3): 655-679.

Waldron J (2012) Constitutionalism: A skeptical view. Report by NYU School of Law, Public Law Research Paper No. 10-87. Available at SSRN: https://ssrn.com/abstract=1722771

Waz J and Weiser P (2013) Internet governance: The role of multistakeholder organizations. *Journal of Telecommunications and High Technology Law* 10(2): 331-350.

Williams G (2006) The Victorian Charter of Human Rights and Responsibilities: Origins and scope. *Melbourne University Law Review* 30(3): 880-905.

Williams G and Reynolds D (2016) A Human Rights Act for Queensland? Lessons from recent Australian experience. *Alternative Law Journal* 41(2): 81-85.

Yilma, K (2017) Digital privacy and virtues of multilateral digital constitutionalism – preliminary thoughts. *International Journal of Law and Information Technology* 25(2): 115-138.

York J (2014) Statement on the use of Finfisher by members of the Freedom Online Coalition. In *EFF Deeplinks Blog*. Available at: https://www.eff.org/deeplinks/2014/09/statement-use-finfisher-members-freedom-online-coalition

Zedner L (2009) *Security.* London and New York: Routledge.