Article

Technology, Law, and the Formation of (II)Liberal Democracy?

Adam Molnar

Deakin University, Australia.
adam.molnar@deakin.edu.au

Abstract

This article argues that the politics of surveillance in Australia is conditioned by the dynamic interplay between law and technological developments. Applying criminologist Richard Ericson's concept of 'counter-law', the article illustrates how rapidly advancing capacities for surveillance and Australia's legal infrastructure collide. In this view, even regulatory safeguards can be instrumental in an authoritarian drift in liberal democracy. Drawing on the Australian context to illustrate a broader trend in Western liberal democracies, this article conveys how such an apparatus of control specific to liberal democracy might be more accurately understood as a form of socio-technical rule-with-law.

Introduction

In a recent article titled, '*The Assault on Australian Democracy*', it was noted that some 350 instances of laws in Australia hold serious potential to encroach upon rights and freedoms essential to the maintenance of a healthy democracy (Williams 2016). Williams' systematic review of federal, state, and territory statute books is unnerving. Notably, of these 350 laws, 209 were enacted in the short time since 9/11 (Williams 2016: 27). 64 of these statutes are specific to anti-terrorism measures, indicating the extent to which 9/11 has had an influence on the making of Australian laws. While many of these laws do not refer directly to authorising surveillance activities, the investigation and 'enforcement' of these infractions *are* dependent on the administration of increasingly vigorous regime of surveillance. Australia's turn to what Williams calls "a shallow adherence to freedom of speech, and an unwelcome, authoritarian streak on behalf of the government and the opposition" (2016: 41), is augmented by a strong appetite for surveillance and control, illustrated by Australia's turn to a national facial biometrics program (Mann and Smith 2017), mandatory data retention requirements and warrantless access to stored telecommunications that undermine human rights norms (Suzor, Pappalardo and McIntosh 2017), and sweeping authorities to conduct computer network operations (Molnar, Parsons and Zouave 2017). In conjunction with these legal encroachments on democratic values, a significant part of this trajectory has been compounded by the lawful sanctioning of secrecy (Hardy and Williams 2014), which diminishes transparency and accountability required for democracy by undermining appropriate degrees of reciprocal visibility between the liberal state and its citizens (Brin 1998; Williams 2016).

While these findings paint a troubling picture about the duress that Australian liberal democracy is currently facing, the aim of this article is to reflect on some less recognised processes that inform how the

infrastructure of the surveillance state in Australia is conditioned through a dynamic interplay at the intersection of law and technological developments. Drawing on criminologist Richard Ericson's concept of 'counter-law' (2006, 2007) to explain this socio-technical dynamic, two key developments in the concept are significant: one that centres on legal developments of the liberal state, and another that centres on technological developments. I argue that the formation of the liberal surveillance state in Australia (though not restricted to this jurisdiction alone) is emerging at the dynamic intersection between these two parallel, yet intersecting, aspects of counter-law. I begin by advancing an analytical framework for illuminating how authoritarian practices of liberal governments are facilitated through a presently-unfolding dynamic at the intersection of liberal rationality of 'rule of law' and technological/surveillance capabilities. I continue with an exploration of how subsequent developments in security and policing apparatuses in Australia establish conditions for (il)liberal forms of rule. Given the material constraints of this article, I cannot explore other relevant aspects of authoritarian rule: the politics of fascism, particularly as it operates through a contemporary aestheticisation of the political (Martin 1992); the obvious authoritarian implications inherent in sovereign constructions of 'risky' populations as a basis for management (Amoore 2014; Monaghan and Walby 2012); or the goals, interests, norms and habitus of professionals in the management of unease (Bigo and Tsoukala 2008). Rather, I seek to understand how socio-technical-legal apparatuses work to enable or constrain possibilities for authoritarian forms of control.

Socio-technical-legal apparatuses

In *'Crime in an Insecure World'*, Richard Ericson (2007), offers the concept of 'counter-law' as a way to come to terms with the legal and technical/surveillance features of an emerging shape of a regulatory apparatus of control. The first development, which Ericson calls 'Counter-law I', is specific to the legal environment, and it refers to the more recent proliferation of criminal procedure and counter-terrorism statutes, that since 9/11 in particular, have eroded or even eliminated constitutional standards of rule of law. Examples of this development includes opaque legal definitions, the erosion of judicial review in favour of ministerial authorisation, and increasingly lowered thresholds to justify 'pre-crime' interventions—often through practices of surveillance—in the activities of those deemed to be future threats to security and safety. Counter-law I also describes legislative sanctioning of developments that favour mass, undifferentiated, collection and storage of personal information on populations, irrespective of their involvement in criminal activity (McCulloch and Wilson 2016; Zedner 2009).

Ericson's second concept, Counter-law II, refers to the proliferation of an interconnected, networked digital environment that facilitates new ways to identify and control risks and uncertainty associated with criminality (Ericson 2007). The proliferation of surveillance technologies as a ubiquitous feature of our everyday life is all-permeating. Our technological environment provides unprecedented means for governments and the private sector to monitor personal communications and profile behaviours. This phenomenon promises exciting possibilities to solve complex problems, but it also opens the door for increased surveillance, identification, and control (Andrejevic 2012). The ubiquity of the digital environment means that there are few, if any, everyday practices that *do not* involve the creation of at least some sort of 'digital exhaust' or 'data shadow', whereby our most personal behaviours, interests, associations, and geo-locational patterns are mirrored in multiple forms and locations. The technological means that afford control over information and bodies—including bulk data collection, content filtering, targeted malware attacks—reveals the extent to which counter-law II developments are a cornerstone in contemporary manifestations of the management (and creation) of unease.

Insofar as counter-law II is allowed to flourish through the legal grey and black holes afforded in counter-law I developments, we see a double re-drawing of expressions of sovereign authority in the socio-technical apparatus. The first drawing occurs through expansive and permissive scope for operational discretion through counter-law I developments. The second drawing refers to how politics-of-risk through a system of differentiations entail an embedding of forms of 'mis-identification' into technology-facilitated practices of

surveillance (Monaghan and Walby 2012). In counter-law II, a system of differentiations is contingent on constructions of risk and their embeddedness in technological practices (Lyon 2007; Mantello 2016). The security and protection of individuals against authoritarian manifestations under liberal democracies also depends on the security and integrity of information communication infrastructures, and not strictly constraints provided through a system of lawful checks and balances (Deibert 2015; Molnar, Parsons and Zouave 2017: 8). In the absence of measures that provide transparency and accountability in the use of technologies such as algorithms and predictive analytics—which themselves operate as a mystification of representation—become a vital aspect of social control under liberal conditions.

In this era of counter-law, the formation of the liberal surveillance state is emerging precisely where a rapidly proliferating technological environment collides with permissive legislative parameters that struggle to define the reality they are required to reflect. The collision between rapidly advancing capacities of surveillance and unrestrictive, and often outdated, legislation makes for a relatively unconstrained environment for agencies to conduct surveillance and control. Austin (2015a) has termed this development a form of ‘lawful illegality’, whereby the principles and norms of rule of law are increasingly undermined through what may essentially be ‘lawful’ practices. The ‘lawful’ use of surveillance technologies are increasingly understood to open up operational discretion through legal grey holes, or even legal black holes (Austin 2015a; Dyzenhaus 2006). Further, these lawful authorities are then extended through the changing technological environment of counter-law II. The technical and legal infrastructure cohere to form a trend under contemporary liberal democracies that, while still forging a form of ‘lawful’ state practice, nevertheless challenges rule of law that such technical powers are intended to be authorised and constrained through. The result is a form of *socio-technical rule-with-law* that forges a form of ‘lawful’ state practice, inclusive of the presence of legal ‘safeguards’, that ends up working ‘less as a barrier to government power, and more an instrument of its exercise’ (Lippert and Walby 2016: 329).

Counter-law and the formation of the Australian surveillance state

The infrastructure of the surveillance state in Australia is part of both a ‘passive’ and ‘active’ set of socio-legal developments. Counter-law developments are passive, insofar as older legislation is increasingly outpaced by a rapidly evolving technological environment. In Australia’s Federal Surveillance Devices Act (2004) (SDA), warrant categories are broken down by ‘technology-specific’ language: intended to reflect the methods and tactics of investigation and their relation to boundaries of privacy. However, it is unclear how accurately these statutes reflect the manifold capacities of existing surveillance technologies. For example, the SDA attempts to categorise the technologies within a legal framework that relates to degrees of binding constraints for the use of ‘optical surveillance devices’, ‘data surveillance devices’, ‘tracking devices’, and ‘audio surveillance devices’ (SDA 2004). However, surveillance technologies can easily drift in and out of each these categories in the legislation, leading to a disconnect in the legal frameworks that were designed provide specific degrees of democratic checks and balances. For instance, when unmanned aerial vehicles or drones could, in principle, be defined as an optical surveillance device or a tracking device it is unclear what statute the devices should be used under, and by extension, what constraints should apply. In other words, if an optical surveillance device is affixed to a drone, offering persistent aerial vision, it has the same surveillance capacity as a GPS ‘tracking’ device, but which statute does the use of the technology fit under?

While common sense might suggest that having a range of surveillance technologies covered under a breadth of legislation is perhaps a ‘good’ problem to have, an ambivalence between surveillance capacities and legal statutes matters insofar as authorities are able to engage in regulatory arbitrage. Based on a disconnect between technological realities and legal infrastructure, authorities enjoy unbounded discretion to ‘fit’ technologies under statutes based on loose categorical definitions that misapprehend the actual degree of invasiveness and proportionality of the type of surveillance being used. Moreover, technologies and practices of identification can also drift in and out of entire legislative frameworks. The Telecommunications

(Interception and Access) Act 1979 (TIA 1979) provides warrantless access to metadata—including historical geo-locational information—which can *also* function as a tracking technology. ‘Tracking’, as a technologically facilitated surveillance capacity, therefore, can occur under multiple, yet different, lawful requirements, each with varying degrees of constraint. To take an example from Canada, the Royal Canadian Mounted Police (RCMP) relied on a mystifying interpretation of IMSI-catcher technology as a way to use the devices outside Canada’s dominant surveillance legislation. The RCMP interpreted IMSI-catchers as a mobile ‘jamming’ device under the Radiocommunications Act (RSC 1985) instead of a surveillance device under the Criminal Code (RSC 1985). The Radiocommunications Act offered comparatively weak regulatory controls, namely, no requirement to seek judicial authorisation to deploy what is, by definition, an indiscriminate mass surveillance technology (Seglins, Braga and Cullen 2017; Parsons and Israel 2016; Pell and Soghoian 2013: 148).

In Australia, the outstripping of the technological environment against the legal environment as a feature of counter-law also emerges through technology-ambiguous language in the Telecommunications (Interception and Access) Act 1979. As I’ve noted elsewhere (Molnar, Parsons and Zouave 2017), it is unclear what legal definitions, such as a ‘telecommunications device’, may refer to in the technological environment. Does this refer to end-point devices such as a mobile device or a computer? Does it refer to a router, or perhaps even a mobile base station? Given the lack of clear wording in primary legislation, we can see how, even with lawful authority, the interpretation of the scope of surveillance is remarkably flexible, and potentially unfettered. While entirely lawful under liberal democratic procedures, such loose categorical definitions, as they relate to the technological environment, may authorise disproportionate forms of bulk collection that are more closely aligned with (il)liberal practices.

These ambiguities between the double-drawing of the legal environment and the operational space, characterised by ubiquitous techno-visibility, are additionally corrosive insofar as they can also weaken the veracity of information in transparency reports. Government transparency reporting is a primary instrument that liberal democratic governments use to build trust and accountability with citizens regarding their use of surveillance powers (Haggerty and Samatas 2010). As the primary legislative environment breaks down in relation to the technical environment, it becomes increasingly difficult to know how specific investigatory methods can be represented in the data of transparency reports. The reliability that might be drawn from annual reports on such numbers is destabilised, undermining yet another component of preserving transparency, trust, and accountability between citizens and governments.

That said, this is not a simple problem of how outdated legislative statutes are disconnected from more recent technological developments. More recently, laws have been passed that *purposefully* attempt to broaden definitions relating to the technological environment. For instance, in late 2014, Australian amendments to the Australian Security Intelligence Organisation Act 1979 (Cth), changed the legal definition of a ‘computer’ (National Security Legislation Amendment Bill (No.1) 2014 Explanatory Memorandum). The government broadened the definition of a ‘computer’ to include “one or more computers”, “one or more computer systems”, “one or more computer networks”, or “any combination of the above” (ASIO Act 1979: s.4). Through ministerial authorisation from the Attorney-General (ASIO Act 1979: s.25(a)), a single computer access warrant can allow surveillance of entire businesses, university networks, telecommunications companies, or could even include core internet infrastructure for gathering intelligence or disrupting activities (Hardy 2014). This amendment also provides Australian Security Intelligence Organisation (ASIO) an authority to engage in disruption: to use “any other computer or communication in transit to add, copy, delete or alter data...for the purpose of obtaining access to data relevant to the security matter and held on the target computer” (National Security Legislation Amendment Bill (No.1) 2014 Explanatory Memorandum). With the purposeful amendment of primary legislation as part of counter-law I, general warrants are also gaining traction as a feature of criminal procedure in the United States (US) under contemporary counter-law conditions (Tummarello 2017).

'Safeguards' and the surveillance state

Australia, a state without a formal bill of rights, lacks an important mechanism for resolving legal ambiguity between technological and legal codes (Williams 2011). This means that a federally situated mechanism of judicial review that may otherwise provide clarity for legal grey areas in relation to surveillance and the impacts on democratic rights, including privacy, is largely unavailable. Australia's regulatory apparatus of oversight and accountability must rely on primary legislation as a basis to investigate and ensure compliance with surveillance powers. As a result, the actual power and force of Australia's oversight and review bodies are largely premised on the robustness or weaknesses of the primary legislation, which as we've seen, is punctuated by counter-law developments.

Counter-law developments can even ensnare privacy safeguards, which are commonly deferred to as a primary bulwark against unwarranted or excessive surveillance. For instance, Australia's Privacy Act (1988) is a central legal framework for enabling and constraining information sharing between law enforcement and security bodies. However, as yet another instrument dependent on the merits of primary legislation, security intelligence and defence are entirely exempt from its reach. Counter-law I developments in the Privacy Act mean that the law, in this instance, works as an expression of normalised exception. The Act places no limitations on the scope of collection, retention, or information sharing, so long as the management of personal information is "for a law enforcement activity" (Privacy Act 1988). In practice, the Privacy Act functions more as a 'fig-leaf' of symbolic lawfulness rather than an instrument that mediates information sharing (Molnar and Parsons 2016).

Australia does have legislative review bodies; there is the Independent National Security Legislation Monitor, the Australian Law Reform Commission, and there is also the Parliamentary Joint Committee on Human Rights. However, as Williams' (2016) work conveys, the work of these committees and agencies has scarcely been felt in Parliament. The problem, therefore, is a persistent one: laws, as currently written, compel oversight bodies to purely evaluate the 'legality' or 'lawfulness' of surveillance activities and provisions of privacy. As long as government agencies only act within their already permissive legislative mandates, expansive new surveillance activities will be regarded as lawful despite their intrusive potential. The implication is that even forms of 'transparency', 'privacy', and 'safeguards' more generally become less of a barrier to the practice of power, but actually an integral aspect of it (Molnar and Parsons 2016; Lippert and Walby 2016). The principle of Rule of Law and 'democratic safeguards' are not simply norms that are intended to curb potential abuses of power, but instead, and especially under counter-law conditions, form the infrastructure of the liberal surveillance state.

While a formal bill of rights does exist at the State level in Victoria, it too is engaged in counter-law developments. Victoria's bill of human rights lacks necessary measures for interpreting the proportionality of surveillance operations (Molnar, Parsons and Zouave 2017: 8). The bill of rights even includes an exception which allows law enforcement to use surveillance methods even if they threaten to impact innocent third parties, so long as those operations are performed "in accordance with procedures, established by law" (Charter of Human Rights and Responsibilities Act 2006: s.21(3)). In Victoria, even with a bill of rights present, civic protections are almost entirely dependent on the capacities of parliaments to draft laws that might uphold a system of human rights. The juridical 'safeguarding' of human rights are therefore clearly incorporated into the limits provided under primary legislation.

Even in jurisdictions with a formal bill of rights, such as Canada and the US, constitutional protections are under serious strain. Insofar as an 'individual expectation of privacy' has become a dominant metric through which to evaluate liberal constitutional protections, courts often defer protections against intrusive surveillance on the basis that information is not sufficiently related to one's own "biographical core" (Austin 2015b) or that the information has already been made available to third party intermediaries which shifts 'reasonable' expectations about confidentiality and possibilities for future access to information. For

instance, US third-party doctrine permits warrantless access to personal information insofar as this information has already been voluntarily disclosed to third party entity through a private contract. Moreover, given the persistent ‘exceptionality’ of state surveillance as a response to a ‘catastrophic risk’ of terrorism, the liberal calculus for assessing constitutional constraints of necessity and proportionality are prone to consistent erosion (Austin 2015b). In the context of low-risk, yet high-impact events such as terrorism, protections are often traded away in the name of ‘collective security’. ‘Terrorism’ is also a compelling basis to acquire technologies that regularly creep into routine criminal law enforcement operations (Cushing 2014).

However, rights-based constitutions are also able to be circumvented through Counter-law II developments. In the US, the use of ‘traffic shaping’—a technique designed to “deliberately divert” US internet traffic—allows the National Security Agency (NSA) to shape the geographical trajectory of digital communications in ways that circumvent constitutional constraints that are intended to prevent domestic mass surveillance of American citizens (Goldberg 2017). The purposeful manipulation of internet infrastructure creates a legal exception to facilitate arbitrary scope for the NSA to collect bulk data, inclusive of both foreign and US citizens without valid warrant requirements. Notably, it wasn’t until the disclosures from Edward Snowden that this tactic was more explicitly revealed, indicating the extent to which secrecy and obfuscation work as an additional feature of the liberal surveillance state.

The punitive force of secrecy

More recent legislation to enhance governmental secrecy and anti-whistleblower laws in Australia further limit possibilities through which democratic rights might be respected. While a thorough review of Australia’s oversight, accountability, and secrecy regime is beyond the scope of this article, it is worthwhile to note how counter-law developments also include measures that impose significant limits to transparency and accountability. For instance, if ASIO activities are designated as a “special intelligence operation” (SIO) by the Attorney-General (ASIO Act 1979: s.35(b)), ASIO officials (and deputised affiliates) are provided civil and criminal immunity (Hardy and Williams 2016; ASIO Act 1979: s.35(k)). A five-year penalty exists if any information about an SIO is disclosed by any citizen, for any purposes, and whether knowingly or not. This penalty can be extended to 10 years if the disclosure is found to “endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation” (ASIO Act 1979: 35(p)). This statute is understood by the Attorney-General to apply “generally to all citizens” (Williams 2016): including journalists and whistle-blowers. Similarly, Section 70 of the Crimes Act states that any disclosure of a surveillance operation, found to be “prejudicial to the effective working of government”, by any current or former Commonwealth officer, is punishable by imprisonment for up to 2 years (Hardy and Williams 2014: 802; Crimes Act 1914: s.70). Similarly, the Border Forces Act 2015, places a two-year penalty of imprisonment on government employees and contractors who disclose any information that could be proven to damage the state (Border Forces Act 2015: s.42). Where protection from (il)liberal practices are also dependent on the security and integrity of information communication infrastructures, it is also possible that excessive secrecy regimes can be found to undermine policies like a public vulnerability equities reporting process.

Conclusion

In spite of emphasising the regulatory force of ‘Law’, I do not intend to ascribe a mythological force to law as an entity that stands outside the social. A redrawing of the boundaries of law will not *necessarily* limit our present drift into (il)liberal practices of liberal regimes. Indeed, liberal settler colonial societies are already premised on a scaffolding of liberal individualising practices and ‘mentalities of rule’. As such, they are always-already inherently authoritarian (Wolfe 2006; Blomley 2003). However, I argue that counter-law developments more readily reveal the extent to which ‘lawfulness’ as a counter-balance to authoritarian trends of the liberal surveillance state is a rather deceptive yardstick under current technological conditions.

Law, insofar as it defines a “form of general intervention excluding particular, individual, or exceptional measures” (Foucault 2008: 321) largely exists as a normative register that opens up myriad possibilities for (il)liberal forms of technology-facilitated surveillance and control. In spite of oft-heard appeals to the ‘lawfulness’ of state surveillance and disruption, a ‘post-legal’ space of routinised exceptionality emerges at the intersection of law and technology. As a systematic feature of control in liberal democracies, such ‘lawful’, yet unbounded ‘post-legal’ terms (Bowling and Sheptycki 2014) can be recognised in Australia (in particular) through government use of computer network operations (Molnar, Parsons and Zouave 2017), unbounded emergence of biometric facial recognition (Mann and Smith 2017), or warrantless access to metadata and compulsory mandatory data retention (Suzor, Pappalardo and McIntosh 2017).

It is increasingly clear that authoritarian impulses, specific to an economy of surveillance and control under liberal democracies, rely not only on the extent to which the aesthetics of the Other are enmeshed in what are often technology-facilitated practices of control. They also rely upon a subtler dynamic between an actual and symbolic register of ‘lawfulness’ as it relates to proliferating technical capacities of surveillance and control. Such an apparatus of counter-law, as an expression of the liberal surveillance state, might be more accurately understood as a form of *socio-technical-rule-with-law*.

References

- Amoore, Louise. 2014. “Security and the Claim to Privacy.” *International Political Sociology* 8(1):108-112. doi:10.1111/ips.12044.
- Andrejevic, Mark. 2012. “Ubiquitous Surveillance.” In *Routledge Handbook of Surveillance Studies*, edited by Kirstie S. Ball, Kevin Haggerty, and David Lyon, 91-98. New York: Routledge.
- Austin, Lisa M. 2015a. “Lawful Illegality: What Snowden has Taught us About the Legal Infrastructure of the Surveillance State.” In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 103-126. Ottawa, ON: University of Ottawa Press.
- Austin, Lisa M. 2015b. “Surveillance and the Rule of Law.” *Surveillance & Society* 13(2):295-299. <http://search.proquest.com/openview/95181f928df3a9e51e6f44ba187ad4d0/1?pq-origsite=gscholar>.
- Australian Security Intelligence Organisation Act 1979 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_act/asioa1979472/.
- Bigo, Didier, and Anastassia Tsoukala. 2008. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. New York: Routledge.
- Blomley, Nicholas. 2003. “Law, property, and the geography of violence: The frontier, the survey, and the grid.” *Annals of the Association of American Geographers* 93(1): 121-141. doi:10.1111/1467-8306.93109.
- Border Forces Act 2015 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_act/abfa2015225/.
- Bowling, Ben, and James Sheptycki. 2014. “Global Policing, Mobility and Social Control.” In *The Routledge Handbook on Crime and International Migration*, edited by Sharon Pickering, and Julie Ham, 57-74. New York: Routledge.
- Brin, David. 1998. *The Transparent Society: Will Technology Force us to Choose Between Privacy and Freedom?* New York: Basic Books.
- Canada Criminal Code 1985 (RSC). <http://laws-lois.justice.gc.ca/eng/acts/C-46/>.
- Charter of Human Rights and Responsibilities Act 2006 (Vic). http://www.austlii.edu.au/au/legis/vic/consol_act/cohrra2006433/.
- Crimes Act 1914 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/index.html#s70.
- Cushing, Tim. 2014. “Stingray Documents Show Law Enforcement Using ‘Terrorism’ To Obtain Equipment To Fight Regular Crime.” *TechDirt*, June 2. Accessed April 20, 2017. <https://www.techdirt.com/articles/20140619/09211027625/stingray-documents-show-law-enforcement-using-terrorism-to-obtain-equipment-to-fight-regular-crime.shtml>.
- Deibert, Ron. 2015. “Cyberspace under Siege.” *Journal of Democracy* 26(3):64-78. doi:10.1353/jod.2015.0051.
- Dyzenhaus, David. 2006. *The Constitution of Law: Legality in a Time of Emergency*. Cambridge: Cambridge University Press.
- Ericson, Richard. 2006. “Ten Uncertainties of Risk-Management Approaches to Security.” *Canadian Journal of Criminology and Criminal Justice* 48(3):345-356. doi:10.3138/cjccj.48.3.345.

- Ericson, Richard. 2007. "Security, Surveillance and Counter Law." *Criminal Justice Matters* 68(1):6-7. doi:10.1080/09627250708553271.
- Foucault, Michel. 2008. *The Birth of Biopolitics: Lectures at the Collège de France, 1978-1979*. Edited by Michel Senellart. New York: Palgrave Macmillan.
- Goldberg, Sharon. 2017. "Surveillance without Borders: The 'Traffic Shaping' Loophole and Why It Matters." *The Century Foundation*, June 22. Accessed June 22, 2017. <https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/>.
- Haggerty, Kevin D., and Minas Samatas. 2010. *Surveillance and Democracy*. New York: Routledge.
- Hardy, Keiran. 2014. "Sweeping Security Law Would have Computer Users Surrender Privacy." *The Conversation*, September 16. Accessed May 23, 2017. <https://theconversation.com/sweeping-security-law-would-have-computer-users-surrender-privacy-30041>.
- Hardy, Keiran, and George Williams. 2014. "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism." In *Cyberterrorism: Understanding, Assessment and Response*, edited by Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, 1-23. New York: Springer.
- Hardy, Keiran, and George Williams. 2016. "Executive Oversight of Intelligence Agencies in Australia." In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, edited by Zachary K. Goldman, and Samuel J. Rascoff, 315-342. New York: Oxford University Press.
- Lippert, Randy K., and Kevin Walby. 2016. "Governing through Privacy: Authoritarian Liberalism, Law, and Privacy Knowledge." *Law, Culture and the Humanities* 12(2):329-352. doi:10.1177/1743872113478530.
- Lyon, David. 2007. *Surveillance Studies: an overview*. Cambridge: Polity Press.
- Mann, Monique, and Marcus Smith. 2017. "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight." *University of New South Wales Law Journal* 40(1):1-25. <http://eprints.qut.edu.au/102300/>.
- Mantello, Peter. 2016. "The Machine that Ate Bad People: The Ontopolitics of the Precrime Assemblage." *Big Data & Society* 3(2):1-11. doi:10.1177/2053951716682538.
- Martin, Jay. 1992. "'The Aesthetic Ideology' as Ideology; Or, What Does It Mean to Aestheticize Politics?" *Cultural Critique* 21:41-61. doi:10.2307/1354116.
- McCulloch, Jude, and Dean Wilson. 2016. *Pre-crime: Pre-emption, Precaution and the Future*. New York: Routledge.
- Molnar, Adam, and Christopher Parsons. 2016. "Unmanned Aerial Vehicles (UAVs) and Law Enforcement in Australia and Canada: Governance through 'Privacy' in an Era of Counter-law?" In *Security, Surveillance and Law in Comparative Context*, edited by Randy K. Lippert, Kevin Walby, Ian Warren, and Darren Palmer, 225-247. Cham: Springer International Publishing.
- Molnar, Adam, Christopher Parsons, and Erik Zouave. 2017. "Computer Network Operations and 'Rule-with-Law' in Australia." *Internet Policy Review* 6(3):1-15. doi: 10.14763/2017.1.453.
- Monaghan, Jeffrey, and Kevin Walby. 2012. "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre, and Social Movement Suppression." *Policing and Society* 22(2):133-155. doi:10.1080/10439463.2011.605131.
- National Security Legislation Amendment Bill (No.1) 2014 Explanatory Memorandum. http://www.austlii.edu.au/au/legis/cth/bill_em/nslab12014440/memo_0.html.
- Parsons, Christopher, and Tamir Israel. 2016. "Gone opaque? An analysis of hypothetical IMSI catcher overuse in Canada." Citizen Lab-Telecom Transparency Project // CIPPIC Report. <https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone-Opaque.pdf>.
- Pell, Stephanie, and Christopher Soghoian. 2013. "A Lot More than a Pen Register, and Less than a Wiretap." *Yale Journal of Law and Technology* 16(1):134-171. <http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/4/>.
- Privacy Act 1988 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/.
- Radiocommunications Act 1985 (RSC). <http://laws-lois.justice.gc.ca/eng/acts/R-2/>.
- Seglins, Dave, Matthew Braga, and Catherine Cullen. 2017. "RCMP Reveals use of Secretive Cellphone Surveillance Technology for the First Time." *CBC News*, 5 April. Accessed June 30, 2017. <http://www.cbc.ca/news/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750>.
- Surveillance Devices Act 2004 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_act/sda2004210/.
- Suzor, Nicholas, Kylie Pappalardo, and Natalie McIntosh. 2017. "The Passage of Australia's Data Retention Regime: National Security, Human Rights, and Media Scrutiny." *Internet Policy Review* 6(1):1-16. doi:10.14763/2017.1.454.
- Telecommunications (Interception and Access) Act 1979 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.
- Tummarello, Kate. 2017. "The Fight Against General Warrants to Hack Rages on." *Electronic Frontier Foundation*, May 9. Accessed May 23, 2017. <https://www.eff.org/deeplinks/2017/05/fight-against-general-warrants-hack-rages>.
- Williams, George. 2011. "A Decade of Australian Anti- Terror Laws." *Melbourne University Law Review* 35(3):1137-1151. <http://heinonline.org/HOL/LandingPage?handle=hein.journals/mulr35&div=44&id=&page=>.
- Williams, George. 2016. "The Legal Assault on Australian Democracy." *QUT Law Review* 16(2):19-41. doi:10.5204/qutlr.v16i2.651.
- Wolfe, Patrick. 2006. "Settler Colonialism and the Elimination of the Native." *Journal of Genocide Research* 8(4):387-409. doi:10.1080/14623520601056240.
- Zedner, L. 2009. *Security: Key Ideas in Criminology Series*. New York: Routledge.