COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 76–83
DOI: 10.17645/mac.v5i1.810

Article

Metadata Laws, Journalism and Resistance in Australia

Benedetta Brevini

Department of Media and Communication, The University of Sydney, Sydney, NSW 2006, Australia;
E-Mail: benedetta.brevini@sydney.edu.au

Submitted: 31 October 2016 | Accepted: 2 March 2017 | Published: 22 March 2017

Abstract
The intelligence leaks from Edward Snowden in 2013 unveiled the sophistication and extent of data collection by the United States' National Security Agency and major global digital firms prompting domestic and international debates about the balance between security and privacy, openness and enclosure, accountability and secrecy. It is difficult not to see a clear connection with the Snowden leaks in the sharp acceleration of new national security legislations in Australia, a long term member of the Five Eyes Alliance. In October 2015, the Australian federal government passed controversial laws that require telecommunications companies to retain the metadata of their customers for a period of two years. The new acts pose serious threats for the profession of journalism as they enable government agencies to easily identify and pursue journalists' sources. Bulk data collections of this type of information deter future whistleblowers from approaching journalists, making the performance of the latter's democratic role a challenge. After situating this debate within the scholarly literature at the intersection between surveillance studies and communication studies, this article discusses the political context in which journalists are operating and working in Australia; assesses how metadata laws have affected journalism practices and addresses the possibility for resistance.

Keywords
digital resistance; journalists; metadata; surveillance

Issue
This article is part of the issue "Post-Snowden Internet Policy", edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction

The intelligence leaks from Edward Snowden in 2013 unveiled the sophistication and extent of data collection by the US's National Security Agency and major global digital firms prompting domestic and international debates about the balance between security and privacy, openness and enclosure, accountability and secrecy (Brevini, 2017). While many authors (Andrejevic, 2002, 2013; Lyon, 2014; Van Dijck, 2014) have warned about massive data collection by governments and businesses as a challenge to civil rights, there a need to encourage further public discussion around the world on the chilling effect that these data retention frameworks can have on freedom of the press, on journalists and on their ability to exert their traditional watchdog function (Lashmar, 2016). After situating this debate within the scholarly literature at the intersection between surveillance studies and communication studies, this article discusses the political context in which journalists are operating and working in Australia; assesses how metadata laws have affected journalism practices and addresses the violation of privacy for journalists and the emergence of a resistance.

2. From Surveillance Society to Resistance

Surveillance has been defined as the "collection and analysis of information about populations in order to govern their activities" (Ericson & Haggerty, 2006, p. 3) so the literature coming from surveillance studies becomes of great relevance in investigating the impact of metadata laws on journalism practices.

Yet, because of the unprecedented development of information and communication technologies, surveillance scholars have rightly pointed at the new ubiquitousness and embeddedness of surveillance in every as-

pects of life in current networked societies (Lyon, Haggerty, & Ball, 2012), going much beyond traditional and centralised institutional settings.

As a consequence of the accelerated development of a communication technologies, Mann and Ferenbok (2013) have also explored the possibility for "sousveillance" (Mann & Ferenbok, 2013, p. 19), surveillance from the bottom up, where the surveilled is empowered through technology to fight back and enact change from below through mutual watching and monitoring.

While digital surveillance practices have now been amply studied within surveillance studies, there is still great scope for development in the field of communication studies. In this article, I propose to investigate whether we can detect a space for resistance for journalists working within new metadata frameworks. This space is conceptualised as "field of struggles" (Bordieu, 1983)—a bourdieusian concept—that is helpful in investigating this space for agency.

In the launch edition of a new journal Big Data and Society, Couldry and Powell (2014) developed the argument that a question of agency is paramount to our understanding of big data, thus opening up a new research agenda for investigating not only dominant forms of data power, but also alternative forms of datafication emerging from civil society groups, community organisations, journalists .This study takes up this challenge by focusing specifically on the field of struggle (Bordieu, 1983) where journalists operate.

2.1. The Australian Context

Since the attacks of September 2001, there has been a steady increase in number of national security laws in Australia. Over fifty laws were passed to create new criminal offences, new detention, extended investigative powers for security and police officers, new tools to control people's movements and activities without criminal convictions (Ananian-Welsh & Williams, 2014). There is also a worrying tendency to limit courts' powers to review the legality of government action especially on matters of national security. At the same time, there is a clear trend towards an intensification of government secrecy and an extension of its own powers to limit the public's rights of access to information, thus making court reviews in these areas even more crucial (Human Rights Law Centre [HRLC], 2016).

In this context, the Snowden leaks (Brevini, 2017) and their challenges to state secrets can explain the haste that has characterised discussion and implementation of three major pieces of new national security laws in Australia between 2014 and 2015. As Attorney General George Brandis explained during the reading of the bill amending the Australian Security Intelligence Organisation Act 1979 (ASIO Act) and the Intelligence Services Act 2001 (IS Act), the reform is justified by a clear intent to curb whistleblowing activities:

> As recent, high-profile international events demonstrate, in the wrong hands, classified or sensitive information is capable of global dissemination at the click of a button. Unauthorised disclosures on the scale now possible in the online environment can have devastating consequences for a country's international relationships and intelligence capabilities. (Brandis, 2014)

The newly created metadata laws cannot be properly understood without considering the overall context of increased tightening of national security laws and investments in cybersecurity. In light of this, the Australian government announced in its 2015 budget that it will provide:

> $450 million to strengthen Australia's intelligence capabilities, including updating information technology systems and to counter extremist messaging. This includes $131 million to help the telecommunications sector upgrade its systems to retain metadata for two years. (Australian Government, 2015a)

As I will discuss later, the newly established framework is clearly at odds with a more recent tendency that is emerging in courts throughout Europe and the US and backed by international human rights mandates, where a clearly hostile attitude towards disproportionate digital surveillance is being displayed (see for example, Cannataci, 2016; Kaye, 2015).

3. Data Retention in Australia

The revised Telecommunications (Interception and Access, TIA) Act, passed in 2015, sought to specify "the types of data the telecommunications industry should retain for law enforcement and national security purposes or how long that information should be held". Rapid, ongoing changes occurring in the telecommunications environment have, apparently, "undermined" any systematic access to the tools and data that may be available (The Parliament of the Commonwealth of Australia, 2015a, p. 2). Recognising the variations that exist in the holding and maintenance of types of data in the telecommunications industry, the TIA Act demands the "standardisation" of such records for governmental use (The Parliament of the Commonwealth of Australia, 2015a). It is claimed that previous inconsistencies have impeded governmental efforts to "investigate and to prosecute serious offences" (The Parliament of the Commonwealth of Australia, 2015a).

Both houses have, therefore, passed this Bill, which oversees the implementation of a national data retention scheme. This scheme compels telecommunications service providers to "retain, for two years, particular types of telecommunications data" (The Parliament of the Commonwealth of Australia, 2015a).

The TIA Act cites several recommendations delivered by the Parliamentary Joint Committee for Intelligence and Security (PJCIS) as the basis for its framework, including that:

- the data retention obligation only applies to telecommunications data (not content) and internet browsing is explicitly excluded;
- service providers are required to protect the confidentiality of retained data by encrypting the information and protecting it from unauthorised interference or access;
- mandatory data retention will be reviewed by the PJCIS by three years after its commencement (The Parliament of the Commonwealth of Australia, 2015a, p. 3).

Telecommunications data, in this instance, has been largely characterised as metadata: that is data excluding "content" (The Parliament of the Commonwealth of Australia, 2015a, p. 7) such as the source and destination of a communication, subscribers' information, date, time and duration of a communication or connection to a service.[1]

The 2015–2016 Budget includes $153.8 million over four years to "support the implementation and ongoing management" of the data retention scheme, including $131.3 million over three years for telecommunications service providers (Australian Government, 2015b).

Access to citizens' metadata is therefore conferred without judicial oversight. No warrant is required by the 21 criminal law-enforcement agencies that have been permitted the capacity to requisition these records (Farrell, 2016; The Parliament of the Commonwealth of Australia, 2015a).

The explanatory memorandum for the TIA Act does, however, set out a "compatibility with human rights" statement, in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011 (The Parliament of the Commonwealth of Australia, 2015a, p. 5). This statement, which is expanded upon over the course of 30 pages, includes certain caveats and safeguards to ensure the Act's compliance with the upholding of basic civil liberties. It therefore assures, among other things, that:

> The Bill…amends the TIA Act to bolster the privacy protections associated with the access to, and use of, telecommunications data. It achieves this by limiting the agencies which may authorise access to telecommunications data, and by providing that agencies' access to, and use of, telecommunications data is subject to comprehensive oversight by the Commonwealth Ombudsman. (The Parliament of the Commonwealth of Australia, 2015a, p. 6)

The statement asserts that the Bill "is compatible with human rights because it promotes a number of human rights". This is, however, followed by the disclaimer that "to the extent that (the Bill) may also limit human rights, those limitations are reasonable, necessary and proportionate" (The Parliament of the Commonwealth of Australia, 2015a, p. 36).

4. TIA Act and Its Impact on Journalists

In 2015, an amendment to the proposed TIA Act was put forward in the wake of concerns about how a data retention scheme might affect the media. It was recognised that a data retention scheme could "adversely affect" the media's capacity "to provide accurate and reliable information" (The Parliament of the Commonwealth of Australia, 2015b, p. 33) and leave sources vulnerable. The House of Representatives, thus, agreed to the implementation of a "journalist information warrant" regime, which prohibits agencies from "making authorisations to access journalists or their employers' data for the purpose of identifying a confidential source unless a journalist information warrant is in force" (The Parliament of the Commonwealth of Australia, 2015b, p. 33). This also means that journalists' metadata can always be accessed unless the agency is seeking data specifically for the purpose of identifying a journalist's source.

It is at the discretion of an "issuing authority" to issue or refuse the authorisation of a journalist information warrant, based on their understanding of the public interest (The Parliament of the Commonwealth of Australia, 2015a, p. 79). Issuing authorities are judicial officers approved by the minister or members of the Administrative Appeals Tribunal, or lawyers who are appointed by the minister.

It should also be noted that in the case of ASIO, it will be the minister that will issue the warrant. (The Parliament of the Commonwealth of Australia, 2015a, p. 33). According to the law, information warrants will be issued only when the "public interest in the issue of the warrant outweighs the public interest in maintaining the confidentiality of the source" (The Parliament of the Commonwealth of Australia, 2015a, p. 33).

The installation of (a) Public Interest Advocate(s) should be an additional measure by which the Act seeks to establish independence (The Parliament of the Commonwealth of Australia, 2015a, p. 33). The Public Interest Advocate can make submissions to requests for journalists' data, defending the need to maintain or discard

[1] In January 2016, Australian Privacy Commissioner Timothy Pilgrim appealed a decision of the Administrative Appeals Tribunal (Telstra Corp Ltd and Privacy Commissioner [2015] AATA 991 of 8 December 2015) that mobile phone metadata held by telecom provider Telstra were not "personal information" about its customers under the Australian Privacy Act 1988 This appeal has given the Federal Court a landmark opportunity to establish whether metadata constitutes personal information thus redefining data protection law in Australia. In 19 January 2017 the Federal Court has closed the case and delivered a groudbreaking decision that will have long lasting implications on how metadata is understood by Australians, and the access private citizens will be granted to their own data and digital trails: the Court decided that the mobile phone in question was not "personal information", effectively enshrining this interpretation into law and drastically narrowing the definition of "personal information" under the Privacy Act.

confidentiality, which the minister must consider as a part of the warrant's application. These may include conditions and/or restrictions (The Parliament of the Commonwealth of Australia, 2015a, p. 83). The Public Interest Advocate will, however, not be allowed to seek the advice of media entities, be it the journalist or the organisation, addressed in the journalist information warrant (Keane, 2015a). Indeed, the status of journalists and media organisations as parties subject to a warrant will not be permitted for disclosure (Keane, 2015a). It is so secret that there are two-year jail terms for disclosure, of the mere existence or non existence of a journalist information warrant, while journalists will not be informed of the request being pursued.

It is difficult not to see the flaws in this system and its detrimental effects on the practice of journalism. The journalist information warrant operates in secret, while journalists and their media organisation will never know if access was granted. It will still allow journalists' metadata to be accessed to identify a journalist's sources, while the public interest advocates won't be able to argue in defence of the public watchdog role of news organisation and their responsibility to protect the identity of a source. As journalist Laurie Oakes recalled: "metadata collection is the great press freedom issue of the internet age". The aggressive attitude towards whistleblowers means that governments "now hunt down those leakers with zeal and this means that metadata is their friend" (Oakes, 2015).

5. From Metadata Laws to Special Intelligence Operations Reform: Targeting Journalist's Sources

As discussed, the metadata retention scheme enforced by TIA 2015 has obvious consequences not only for journalists but for their sources, and whistleblowers. However, TIA, combined with another amendment of Australian National Security laws, specifically section 35P of the ASIO has even a greater detrimental impact on journalists' sources.

Under Section 35P of the ASIO Act 1979, those who have "disclosed information relating to a special intelligence operation" may be imprisoned for five to ten years (The Parliament of the Commonwealth of Australia, 2014, p. 71). A "special intelligence operation" can be understood as operations where ASIO agents are granted legal immunity for engaging in a range of otherwise criminal conduct. The most "basic" breach, in which information is simply disclosed, can result in a five-year penalty. Where a disclosure endangers "the health or safety of a person", the Act permits a penalty of ten years. This penalty applies regardless of whether the citizen or journalist in question is aware of an operation's status.

In a report commissioned by the Department of the Prime Minister and Cabinet (DPMC), the impact of this piece of legislation is suggested to be twofold: a gag order like 35P may instil a "chill effect" on publications about the activities of ASIO, and prevent "reprehensible conduct" by ASIO insiders from being susceptible to public scrutiny (DMPC, 2015). According to the report, such an impact is "unjustified" despite the need for secrecy in many ASIO operations. The inadequate protection of the rights of "outsiders", it argues, "infringes the constitutional protection of freedom of political communication" (DPMC, 2015). This new provision is concerning for a number of reasons. First, without an explicit verification from ASIO, it is extremely difficult for a journalist to know whether an ASIO operation is a special intelligence operation or not. Additionally, the new section criminalises both intentional and reckless disclosure, so journalists are likely to take a conservative approach to publication and avoid pursuing reporting of ASIO's activities for fear of being prosecuted. This will indeed lead to a progressive self-imposed censorship of journalists and a progressive lack of public reporting in formal publications or through anonymous disclosures and scrutiny of intelligence activities.

As the controversy around Australian asylum seekers policy arose, in 2015,[2] the Australian Government expanded secrecy laws frameworks and penalties for whistleblowers through the controversial Border Force Act. The legislation makes it unlawful for a Department of Immigration and Border Protection's employee or contractor, such as a social worker, a nurse, a doctor or welfare services provider, to disclose or record certain information obtained while carrying out their duties. The penalty for such a disclosure is up to two years in jail (HRLC, 2015).

As The Guardian's Paul Farrell commented:

> This is a move that should alarm all citizens. It's not an attack on any particular news outlet. It's an attack on those who have reported on matters of significant public interest in the increasingly secretive area of asylum seeker policy….These kind of attacks [sic] severely damage the confidence between reporters and their sources and pose a grave threat to effective and responsible journalism. When the federal police go knocking on the doors of a reporter's sources, sources will soon dry up. People will be scared. And that is exactly the point. (Farrell, 2015)

It is important to note that the Border Protection Act has been amended in October 2016 exempting health professionals from the definition of "immigration and border protection workers" following the pressures coming from the health professionals who challenged the Government in the High court (Hall, 2016). However, the current ban remains in place for others, such as child protection workers and teachers, who witnessed abuses in offshore detentions (Hall, 2016).

[2] For a good summary of controversial Australian Asylum policies and United Nations (UN) criticism please, see "Australia Asylum: Why Is It Controversial?" available at http://www.bbc.com/news/world-asia-28189608

6. A Look at the Current International Context

The newly established metadata scheme regime clearly posits new challenges not only for journalism practices but for the effectiveness of shield laws which are meant to prevent journalists from being forced to reveal their sources. It is also quite unclear how the current Australian national framework for data collection corresponds to, or addresses, existing international conventions, treaties or policies on free speech, political, economic and cultural inclusion. For example the European Court of Justice in April 2014 invalidated the EU's Data Retention Directive, which is very similar to the Australian scheme. In particular, "the Court held that the Directive entailed serious interference with the rights to privacy and personal data protection of individuals guaranteed by the Charter of Fundamental Rights, and also failed to establish limits on access by competent national authorities, such as prior review by a judicial or an independent administrative authority" (Data Retention Directive, 2014). The lack of safeguards around the access and use of metadata was a key reason for the directive to be in breach of the fundamental right to privacy.

Australia's attitude towards metadata frameworks is not unique in international settings. The first report issued by the UN rapporteur on privacy has noted that the country monitoring process of the last year has "revealed several examples of legislation being rushed through national parliaments in an effort to legitimise the use of certain privacy-intrusive measures by Security and Intelligence Services (SIS) and law enforcement agencies" (Cannataci, 2016, p. 6). Moreover, the report notes that there is a contradictory trend between governments and international attitude towards metadata regimes:

> The tensions between security, corporate business models and privacy continue to take centre stage but the last twelve months have been marked by contradictory indicators: some governments have continued, in practice and/or in their parliaments to take privacy-hostile attitudes while courts world-wide but especially in the USA and Europe have struck clear blows in favour of privacy and especially against disproportionate, privacy-intrusive measures such as mass surveillance or breaking of encryption. (Cannataci, 2016, p. 21)

The stand of the mandate of the International rapporteur on Privacy (Cannataci, 2016) is consistent with the indications of the UN, voiced by the former Rapporteur for Freedom of Information Frank La Rue.

> National data retention laws are invasive and costly, and threaten the rights to privacy and free expression. By compelling communications service providers to create large databases of information about who communicates with whom via a telephone or the Internet, the duration of the exchange, and the users' location, and to keep such information (sometimes for years), mandatory data retention laws greatly increase the scope of State surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to theft, fraud and accidental disclosure. (La Rue, 2013, p. 18)

The recommendations of the Rapporteur are clearly at odds with the newly approved Australian framework:

> Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law. (La Rue, 2013, p. 21)

7. Metadata Laws: Is There Room for Journalists' Resistance?

I have argued elsewhere (Brevini, 2017) that the revelations by whistleblower Edward Snowden triggered the birth of a new "new culture of disclosure" that has seen journalists, lawyers and software developers coming together to develop secure online protections and security of their sources. One of the most famous examples are Secure Drop and GlobaLeaks (Brevini, 2017) projects that aim at supporting the practice of whistleblowing by giving people the software tools necessary to start their own initiative. Unlike WikiLeaks (Brevini & Murdock, 2013), GlobaLeaks is an open-source software provider whose intentions are focussed on providing a platform for whistleblowers to use. GlobaLeaks does not handle any leaked documents but assists in the potential creation of whistleblowing sites such as OpenLeaks, MafiaLeaks, BalkanLeaks and BrusselsLeaks. However, there is also a more mainstream response to metadata laws: The New Yorker, the US not-for-profit investigative newsroom ProPublica, the Pierre Omidyar-backed start-up The Intercept and The Guardian are just a few examples of news providers that implemented a newly created open-source whistleblowing platform-SecureDrop to guarantee protections for their sources (Brevini, 2017).

In Australia,[3] the only platform of this kind is mediadirect.org, a platform that aims to encourage encrypted

[3] The paper adopted a multilayered methodological approach that combines policy and legal analysis with interviews with ten investigative Journalists in Australia that prefer to keep their anonymity.

disclosure by anonymous whistleblowers, thus protecting sources from the newly enhanced metadata laws. With a budget of about US$ 3,000 (Interview B)[4] the platform through encrypted interactions connects whistleblowers, who access it via the Tor network, and journalists (Keane, 2015b).

In light of the new metadata frameworks implemented in Australia, one would expect journalists rushing to demand an improved set of encryption tools, as well as formal training on anonymity mechanisms to protect their sources. However, our findings confirm not only a lack of knowledge of encrypting communications but also a lack of understanding of the risks of the newly established frameworks (Interview A, 2016).[5]

As one security consultant revealed:

> In a recent example, I just set them up to deal with the data, because they did not know how to deal with a major data leak. And when I got in there for the first meeting, one of the journalists said, "We'll print everything out". And I'm shocked: it's a million pages and hundreds of thousands of emails, how can we possibly print them? (Interview B, 2016)

Improving journalists' knowledge of encryption tools and their awareness of metadata laws should be a priority for media organisations, and perhaps one of the goals for Media Entertainment Alliance Australia.

Interviewees seemed to agree that the reasons for media institutions not to invest in security tools and training for their journalists has to do with the current financial crisis of journalism and the precarious conditions of reporters: when faced with the clear risk of losing their job, journalists are less keen to take risks and expose wrongdoings.

8. Conclusion

The newly established metadata scheme regime in Australia clearly undermines the work of journalists and the effectiveness of shield laws which were due to protect journalists from being forced to reveal their sources. As Crikey journalist Bernard Keane noted: "The threat arises from the existence and maintenance of data. That creates the chilling effect. You don't need a warrant to investigate a journalist if the agency can access the data of the whole department that the leak came from" (Keane 2015a).

The chilling effect on journalists and whistleblowers' activities are very consistent with findings of the scholarship in surveillance studies that have detected for example a similar pattern of "self censorship" on activists's or civil society groups' activities (see for example, Starr, Fernandez, Amster, Wood, & Caro, 2008).

There are obviously limits to what encryption and anonymity technologies can do to protect journalism practices, but the Australian case certainly shows that, aside from a few exceptions, journalists are currently not well equipped with the necessary know-how and awareness. In Bordieu's terms, journalists in the Australian context have not fully developed the resources or "capital" (Bordieu, 1983) to successfully oppose the collection and processing of personal data, thus developing a space for resistance to surveillance, radically different from "sousveillance" (Mann & Ferenbok, 2013).

It should also be noted that the findings of this study diverge from a recent study by Mills and Sarikakis (2016) that focused only on investigative journalists and found how investigative journalist in Western and non Western countries are engaging increasingly with technological and other communities to defend their work. Future research from Communication Studies perspective should engage with this recent scholarship to shed light on the crucial interplay between new metadata frameworks and journalism.

Conflict of Interests

The author declares no conflict of interests.

References

Ananian-Welsh, R., & Williams, G. (2014). New terrorists: The normalisation and spread of anti-terror laws in Australia. *The Melbourne University Law Review*, *38*, 362–408.

Andrejevic, M. (2002). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479–497.

Andrejevic, M. (2013). *Infoglut: How too much information is changing the way we think and know*. Oxford: Routledge.

Australian Information Commissioner. (2015). Ben Grubb and Telstra Corporation Limited. *Austlii*. Retrieved from http://www.austlii.edu.au/au/cases/cth/AICmr/2015/35.html

Bourdieu, P. (1983). The field of cultural production, or: The economic world reversed. *Poetics*, *12*(4/5), 311–356.

Brandis, G. (2014). National Security Legislation Amendment Bill (No. 1) 2014, Second reading. *Parliament of Australia*. Retrieved from http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=CHAMBER;id=chamber%2Fhansards%2F232fa1a8-d7e8-4b22-9018-1a99b5a96812%2F0116;query=Id%3A%22chamber%2Fhansards%2F232fa1a8-d7e8-4b22-9018-1a99b5a96812%2F0173%22

Brevini, B. (2017). WikiLeaks: Between disclosure and whistle- blowing in digital times. *Sociology Compass*, *1*(3), 1–11.

Brevini, B., & Murdock, G. (2013). Following the money: WikiLeaks and the political economy of disclosure. In

[4] Interview via Skype, 10 May 2016.
[5] Interview via Skype, 3 May 2016.

B. Brevini, A. Hintz, & P. McCurdy (Eds.), *Beyond WikiLeaks: Implications for the future of communications, journalism and society* (pp. 35–55). Basingstoke: Palgrave Macmillan.

Cannataci, J. A. (2016). Report of the special rapporteur on the right to privacy. *Human Rights Council*. Retrieved from www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

Couldry, N., & Powell, A. (2014). Big data from the bottom up. *Big Data & Society*, *1*(2). doi:10.1177/2053951714539277

Data Retention Directive. (2014). *European Union: ECJ invalidates data retention directive*. Retrieved from http://www.loc.gov/law/help/eu-data-retention-directive/eu.php

Department of the Prime Minister and Cabinet. (2015). *Report on the impact on journalists of section 35P of the ASIO Act*. Retrieved from https://www.dpmc.gov.au/pmc/publication/report-impact-journalists-section-35p-asio-act

Ericson, R. V., & Haggerty, K. D. (2006). *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Farrell, P. (2015). Journalism is not a crime. So why are reporters being referred to police? *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2015/jan/22/journalism-is-not-a-so-why-are-reporters-being-referred-to-police

Farrell, P. (2016). Lamb chop weight enforcers want warrantless access to Australians' metadata. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/jan/19/lamb-chop-weight-enforcers-want-warrantless-access-to-australians-metadata

Hall, B. (2016). 'A huge win for doctors': Turnbull government backs down on gag laws for doctors on Naurus and Manus. *Sydney Morning Herald*. Retrieved from http://www.smh.com.au/federal-politics/political-news/a-huge-win-for-doctors-turnbull-government-backs-down-on-gag-laws-for-doctors-on-nauru-and-manus-20161019-gs6ecs.html

Human Rights Law Centre. (2016). *Safeguarding democracy*. Retrieved from http://www.bmartin.cc/dissent/documents/rr/HRLC16.pdf

Kaye, D. (2015). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. *Human Rights Council*. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361

Keane, B. (2015a). Finally the Labor coalition surveillance deal revealed. *Crikey*. Retrieved from http://www.crikey.com.au/2015/03/19/finally-the-labor-coalition-surveillance-deal-revealed/?wpmp_switcher=mobile

Keane, B. (2015b). Media direct: Towards better security for whistleblowers. *Crikey*. Retrieved from https://www.crikey.com.au/2014/05/26/media-direct-towards-better-security-for-whistleblowers

La Rue, F. (2013). Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. *United Nations Human Rights*. Retrieved from http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40

Lashmar, P. (2016). No more sources? The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*. doi:10.1080/17512786.2016.1179587

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In D. Lyon, K. D. Haggerty, & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 1–12). Oxford: Routledge.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13.

Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*, *11*(1/2), 1–13.

Mills, A., & Sarikakis, K. (2016). Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism. *Big Data & Society*, *3*(2), 1–13.

Oakes, L. (2016). *Speech delivered at the Melbourne Press Club, 27 September 2015*. Retrieved from http://www.melbournepressclub.com/wp-content/uploads/2015/09/150925_Melbourne_Press_Freedom_Dinner_Oakes_speech.pdf

The Parliament of the Commonwealth of Australia. (2014). National security legislation amendment bill (No. 1) 2014: Bill as passed by both houses. *Parliament of Australia*. Retrieved from http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s969

The Parliament of the Commonwealth of Australia. (2015a). Telecommunications (Intercept and Access) Amendment (Data Retention) Bill 2015: Revised explanatory memorandum. *Parliament of Australia*. Retrieved from http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375

The Parliament of the Commonwealth Australia. (2015b). Data Retention Bill: Budget Review 2015–16. *Parliament of Australia*. Retrieved from http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/BudgetReview201516/Telco

Australian Government. (2015a). *Budget 2015*. Retrieved from http://www.budget.gov.au/2015-16/content/highlights/nationalsecurity.html

Australian Government. (2015b). *Budget 2015–16* (Budget Paper no.2). Retrieved from http://www.budget.gov.au/2015-16/content/bp2/download/BP2_consolidated.pdf

Privacy Commissioner. (2015). Privacy Commissioner lodges appeal to Federal Court re Telstra Corporation Limited v Privacy Commissioner. *Office of the Australian Information Commissioner*. Retrieved from https://www.oaic.gov.au/media-and-speeches/state

ments/privacy-commissioner-lodges-appeal-to-federal-court-re-telstra-corporation-limited-v-privacy-commissioner

Starr, A., Fernandez, L. A., Amster, R., Wood, L. J., & Caro, M. J. (2008). The impacts of state surveillance on political assembly and association: A socio-legal analysis. *Qualitative Sociology*, *31*(3), 251–270.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

About the Author

Benedetta Brevini is Senior Lecturer in Communication and Media at the University of Sydney, Visiting Fellow of Centre for Law Justice and Journalism at City University and Research Associate at Sydney Cyber Security Network. She is co-editor of the volume *Beyond WikiLeaks: Implications for the Future of Communications, Journalism & Society* (Palgrave MacMillan, 2013) and the author of *Public Service Broadcasting Online: A Comparative European Policy Study of PSB 2.0* (Palgrave MacMillan in August 2013). Before joining academia she has been working as a journalist in Milan, New York and London.