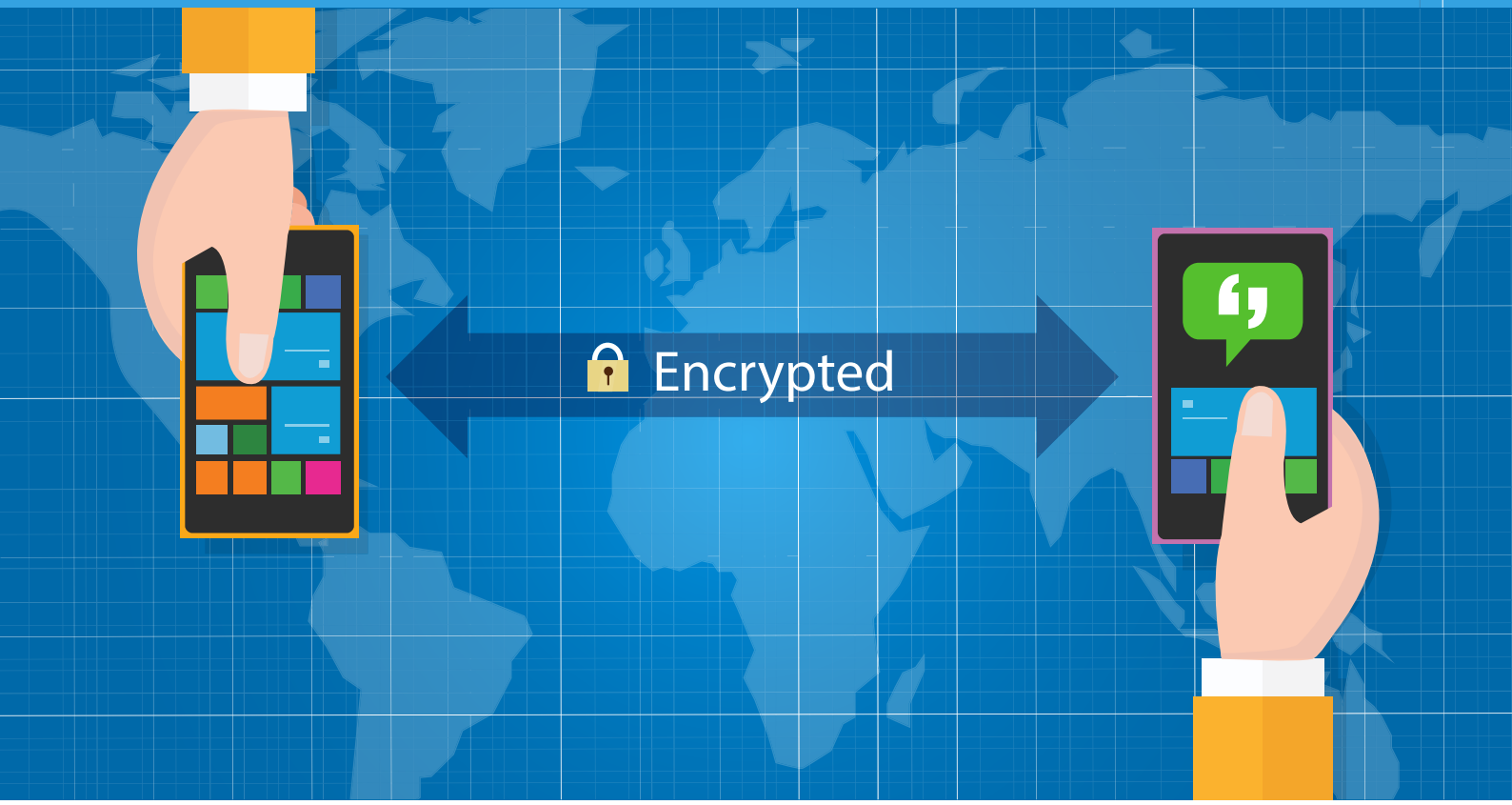
Securing Australian Journalism from Surveillance



DEAKIN UNIVERSITY

ADI
ALFRED DEAKIN INSTITUTE FOR CITIZENSHIP AND GLOBALISATION

Securing Australian Journalism from Surveillance

Dr Diarmaid Harkin & Dr Monique Mann

August 2022

The authors would like to acknowledge the research assistance of Kat Scanlon and Sufian Dilbar in supporting this work. We also appreciate the work of Kathrin Kohl for graphic design. And finally, we wish to extend our gratitude to the journalists, editors, and media lawyers who took the time to support this project.

DEAKIN UNIVERSITY

ADI
ALFRED DEAKIN INSTITUTE FOR CITIZENSHIP AND GLOBALISATION

Executive Summary

- In Australia, the **Data Retention Act (2015)**, the **Assistance and Access Act (2018)**, the **Identify and Disrupt Act (2021)**, and the **International Production Orders Act (2020)** have significantly increased the surveillance powers of law enforcement and intelligence agencies with implications for journalists and the free press.

- This report draws on interviews with 19 journalists and 2 media-lawyers in Australia. The interviews were conducted between May and November 2021. The aim of the interviews was to gauge (a) the level of preparedness amongst journalists in Australia concerning surveillance, and (b) the impacts of increased surveillance powers on journalistic practices.

- There was wide variation in information security understanding and applied skill among media organisations and journalists. Some expressed "very low confidence" (Journalist F) that journalists were adequately prepared for the threats of electronic surveillance and a number conceded that they were not thinking about it "enough" (Journalist Q) or were just "learning on the job but could know more" (Journalist I).

- Some media organisations do not offer support in terms of education and training, policies and procedures, or formal guidance, and even among the most active and equipped organisations, support for cyber security concerns was described as "probably too far down the list of considerations" (Journalist D). In most instances, journalists were self-educating as "it is up to the individual journalist to make sure they are secure" (Journalist A).

- The 2019 AFP raids on the ABC and Annika Smethurst were described as a "holy shit" moment (Journalist P) that raised awareness of government surveillance of journalists. These raids resulted in many journalists and media organisations raising their efforts to protect their digital communications.

- Subsequently, over the past 2 to 3 years many journalists have migrated to encrypted communication applications such as Signal and Protonmail, while several media organisations have implemented SecureDrop for whistle-blowers to provide anonymity and security.

- Journalists suggested media organisations could do more to provide "formalised training" and "organisational support" (Journalist P) and invest more in their employees to provide confidence to potential sources that "journalists are good at this" (Journalist J).

- Participants emphasised that new surveillance laws have had no editorial impacts (i.e., journalists have not avoided stories or covered institutions differently). However, several journalists outlined they have lost sources because they were unable to communicate without leaving digital traces. Likewise, participants reflected that the surveillance laws impacted sources and whistle-blowers and they "are not coming forward as they once did" (Journalist M). As suggested by one journalist, the laws were in place to "fuck over whistle-blowers" (Journalist K) leading to a chilling effect where whistle-blowers were less likely to make disclosures to journalists.

- The enhanced surveillance powers were perceived as a part of a climate of increased antagonism by the (now former) Australian Government against journalism in Australia and this overlapped with concerns around whistle-blowers being aggressively pursued, a developing "culture of secrecy" (Journalist M) in government, and threats of legal proceedings about defamation.

- Journalists had little confidence in the protections for journalists in the metadata retention scheme (i.e., Journalist Information Warrants) or other surveillance laws. These clauses were considered as a "guise — it doesn't actually protect journalists" (Journalist N). Instead, there were calls for judicially authorised warrants for access to the metadata of all Australian citizens or residents.

- There should be enhanced accountability and disciplinary action for when metadata is accessed unlawfully. Some journalists advocated for repealing the electronic surveillance laws while others pointed to greater protections for whistle-blowers in Australia including modifications to public interest disclosure protections and a Media Freedom Act.

- We offer these findings at a critical time of reform of the Australian legal framework governing telecommunications surveillance (see Attorney-General's Department, 2020; Department of Home Affairs, 2021) and present this research and associated recommendations to enhance protections for journalists and the operation of a free press in Australia.

Contents

Acronyms

Administrative Appeals Tribunal (AAT)

Australian Criminal Intelligence Commission (ACIC)

Australian Federal Police (AFP)

Australian Human Rights Commission (AHRC)

Australian Signals Directorate (ASD)

Australian Secret Intelligence Service (ASIS)

Australian Taxation Office (ATO)

Freedom of Information (FOI)

Global Investigative Journalism Network (GIJN)

Independent National Security Legislation Monitor (INSLM)

Internet Services Providers (ISPs)

Journalist Information Warrants (JIW)

Media Entertainment and Arts Alliance (MEAA)

National Security Agency (NSA)

Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Public Interest Advocate (PIA)

Technical Assistance Request (TARs)

Technical Assistance Notices (TANs)

Technical Capability Notices (TCNs)

Introduction

Electronic surveillance poses threats to journalism and requires journalists to consider matters of digital security. A collaboration between media organisations and Amnesty International revealed that at least 180 journalists from 20 different countries "were selected for potential targeting with NSO Spyware" between 2016 and 2021 (Amnesty International 2021). Journalists from the Associated Press, Reuters, CNN, the New York Times, and a range of other outlets are believed to have been targets (ibid). The use of commercial spyware by states is just one example of the type of electronic surveillance journalists now face. Other recent examples include:

- Reporters in Hong Kong are deeply concerned about the extensive surveillance of their devices (Lindberg 2021);
- Australian Federal Police accessing the metadata of journalists as often as 58 times per year (Taylor 2019);
- Reporters in Germany have had a complaint 'admitted for decision' by the European Court of Human Rights into the surveillance practices of the BND (RSF 2021);
- African Digital Rights Network (2021) report significant digital surveillance threats of journalists across ten African countries;
- Foreign correspondents in China report increasing levels of harassment and electronic surveillance (Ping 2019);
- Private investigation agencies such as 'Black Cube' have been contracted to track journalists such as in the case of Harvey Weinstein targeting journalist Ronan Farrow by monitoring the geolocation of his phone (Farrow 2019).

The impacts of electronic surveillance for journalism and a functioning free press have long been identified as a significant issue warranting both academic attention and advocacy. International advocacy groups for journalists such as the *Committee to Protect Journalists*, the *International Consortium of Investigative Journalists*, and the *Freedom of the Press Foundation* have condemned electronic surveillance of journalists and provide guides, training, and advice to journalists about how to improve their digital security.

Scholars have articulated concerns about journalism in the digital era (see for example Ananian-Welsh, 2019; Ananian-Welsh, 2020; Ananian-Welsh, Kendall & Murray, 2021; Murray, Ananian-Welsh & Greste, 2021). There is a focus on how electronic surveillance impacts source protection and whistle-blower ability to securely communicate with journalists (see Eide and Kunelius 2018; Lashmar 2017; Lee and Heinrichs 2019; Posetti 2017). Electronic surveillance and digital monitoring have several impacts on journalism including undermining the ability to protect sources (Lashmar 2017; Posetti 2018), damaging the ability to bring stories to public attention (Lee and Heinrichs 2019; Henrichsen 2020), and otherwise being used to intimidate, deter, and target journalists via harassment and 'incrimination' (Tsui 2019).

Journalists must consider technical questions that intersect with their ability to protect themselves and their sources. They must consider their digital footprint and their traces of communications, documents, movements, and online activities. They must reflect upon how they can keep sources anonymous and how to protect 'data in transit' as they communicate over digital networks, and how to protect 'data at rest' including how to store information long-term. They must develop working knowledge of information security practices around smartphones, laptops, email, location-tracking, file-sharing applications, encryption, messaging services, social media, file metadata, and storage solutions.

These challenges have been recognised in the academic literature focusing on the information security practices of journalists (see for example Di Silvo 2021; Crete-Nishihata et al 2020; Henrichsen et al 2015; Henrichsen 2020; Tsui and Lee 2021). Di Salvo (2021) has explored journalists use of SecureDrop; Crete-Nishihata et al (2020) articulated "information security cultures" developing among investigative and non-investigative journalists; Posetti (2018) outlines digital security strategies undertaken by modern newsrooms; and Tsui and Lee (2021) observe how journalists of higher technical skill tend to enjoy more 'press freedom'.

The contemporary digital landscape has clear impacts for journalists and journalism. It can offer new opportunities for collaborative, international reporting projects (like 'The Panama Papers'). It also offers new ways of connecting and interacting with sources, and advantages for the leaking of classified information in the public interest. However, there are also new threats with governments and other actors capable of surveilling, monitoring, and tracking journalists and their sources. This report explores preparedness of journalists in Australia for responding to the challenge of electronic surveillance and how a raft of recent electronic surveillance laws has made this even more difficult. We offer these findings at a critical time of reform of the Australian legal framework governing telecommunications surveillance (Attorney-General's Department, 2020; Department of Home Affairs, 2021) and make a series of recommendations to enhance protections of journalists and the operation of a free press in Australia.

Part A: Surveillance Laws in Australia and Implications for Journalism

There have been successive legal developments that allow for surveillance of journalists in Australia (see Mann & Murray, 2021 for overview of surveillance legislative developments). This includes the passage of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (herein **'Data Retention Act'**), the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (herein **'Assistance and Access Act'**), the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (herein **'Identify and Disrupt Act'**), and the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* (Cth) (herein **'International Production Orders Act'**). Furthermore, actions by the Australian Federal Police (AFP) against journalists have highlighted issues of surveillance of journalists including the raids of the ABC's offices by the AFP in June 2019 and search of the home of News Corp journalist Annika Smethurst (also by the AFP). These events have been identified by our participants as bringing into sharp attention matters of information security that we explore in this report. This section details the key surveillance legislation and powers that formed the background for this report and unpacks the impacts upon journalism in Australia.

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)

In the lead-up to the introduction of the **Data Retention Act** there was a focus on impacts on journalists and the free press (see Brevini, 2017; Humphreys & de Zwart, 2017; Suzor et al 2017; Keane 2015). Objections were raised by media representatives including the Media Entertainment and Arts Alliance (MEAA) that the retention of metadata was a "dangerous threat to press freedom" and would undermine journalist's ability to protect sources and work "without intimidation, fear or harassment" (MEAA 2015).

The powers required telecommunications companies and Internet Services Providers (ISPs) in Australia to retain telecommunication data for at least 2 years under amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth). The scheme establishes bulk collection of telecommunications data within Australia and permits warrantless access by law enforcement agencies (or any authority declared as a "criminal law-enforcement agency" by the Minister — see section 110A of the *Telecommunications (Interception and Access) Act 1979* (Cth)).

From the perspective of journalists, the **Data Retention Act** has several concerning aspects:

1. **The scheme involves bulk retention of data**. The collection of data is indiscriminate and covers all users of telecommunication services within Australia. Therefore, it will capture individuals who may seek to contact journalists to make public interest disclosures. This could be those who work in public agencies, political parties, companies, NGOs, trade unions, religious institutions, and so on. If sources are not taking

precautions, they will leave digital traces of engagements with journalists such as emails, phone calls, social media interactions, messages, and location data. Journalists must factor this into assurances they make about source protection which has implications for journalists following the MEAA Journalist Code of Ethics' requirement to protect source identity (MEAA 2021).

2. Telecommunications companies and ISPs are **mandated to capture a wide range of data**. The type of information that is retained is sufficiently detailed to make determinations by investigating parties of the time, duration, type, nature, and frequency of communications. ISPs are mandated to collect and store data including but not limited to the "source of a communication", "destination of a communication", the "type of communication" and "location of equipment … used in connection with a communication" (see *Telecommunications (Interception and Access) Act 1979* (Cth) section 187AA).

   It should be noted that section 187A 4(a) of the Data Retention Act articulates that the "contents or substances of a communication" are *not* to be collected and there are assurances in section 187A 4(b)(ii) that "*service providers are not required to keep information about subscribers' web browsing history*." Despite these assurances, the retained information includes the "destination of a communication" which has been interpreted as including "the IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication" (Home Affairs 2021; see section 187AA). Collecting the IP addresses provides information about what websites and servers are visited (e.g., if a person connected to 69.63.176.13 they are browsing Facebook). Many would interpret this as qualifying as "web browsing history" and the Commonwealth Ombudsman reported to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) that telecommunication companies are struggling to manage the "greyness" in the definition of metadata and consequently providing law enforcement agencies with URLs, despite such information *not* being expressly permitted by the scheme (see Taylor 2020a).

   The implication for journalists is that a wide range of data is captured and allows investigating parties to draw inferences and gain significant insights about online activity, location, and the behaviour of both journalists and sources. Furthermore, the Commonwealth Ombudsman has reported that telecommunications companies are storing and sharing data beyond the schemes intended remit (ibid).

3. A **wide range of organisations and individuals are permitted access to the data**. Law enforcement and intelligence agencies enjoy warrantless access to the data (see **figure 1** for a list of agencies with warrantless access). Notably, these agencies are likely to be targets of legitimate journalistic inquiries (e.g., in areas of national security, governmental corruption etc) and are likely to be organisations where journalist's sources work. Therefore, these agencies have considerable power to monitor and police journalistic practices relating to stories that have a direct impact on their own agencies, as was witnessed with the raids on Annika Smethurst's home in response to her reporting on the expansion of the Australian Signals Directorate (ASD) powers to surveil Australian citizens (that indeed came to pass with the introduction of the *Identify and Disrupt Act*).

   Agencies have discretion to appoint "authorising officers" empowered to make requests for metadata. Chief Executive Officers internally appoint "authorising officers" and this can be delegated to low-ranking roles. In principle, agencies are required to have accounting of investigator requests for metadata, but as the Commonwealth Ombudsman's (2021: 3) report into the AFP demonstrated, compliance with internal obligations and adherence to the responsibilities within the Act is low and there is a "cavalier approach to exercising the powers [that] resulted in a culture that did not promote compliance with the TIA Act". Many

individuals within many agencies can potentially misuse these powers and there is limited evidence that internal management procedures ensure the lawful exercise of these powers (and indeed there are many instances of unauthorised access specifically in relation to journalists' information — see for example Commonwealth Ombudsman 2017, 2021).

Furthermore, despite the legislation articulating that metadata ought only to be provided to law enforcement and intelligence agencies (see Section 110A of the Act), in practice a much wider set of organisations have been supplied with access to retained metadata. Disclosures by the Communications Alliance and material obtained by ZDNet under Freedom of Information (FOI) has revealed that at least 87 other organisations have accessed metadata (Taylor 2020b; Duckett 2016). This has included, *inter alia*, the South Australia Fisheries Department, Bankstown City Council, Greyhound Racing Victoria, Racing NSW, and the RSPCA.

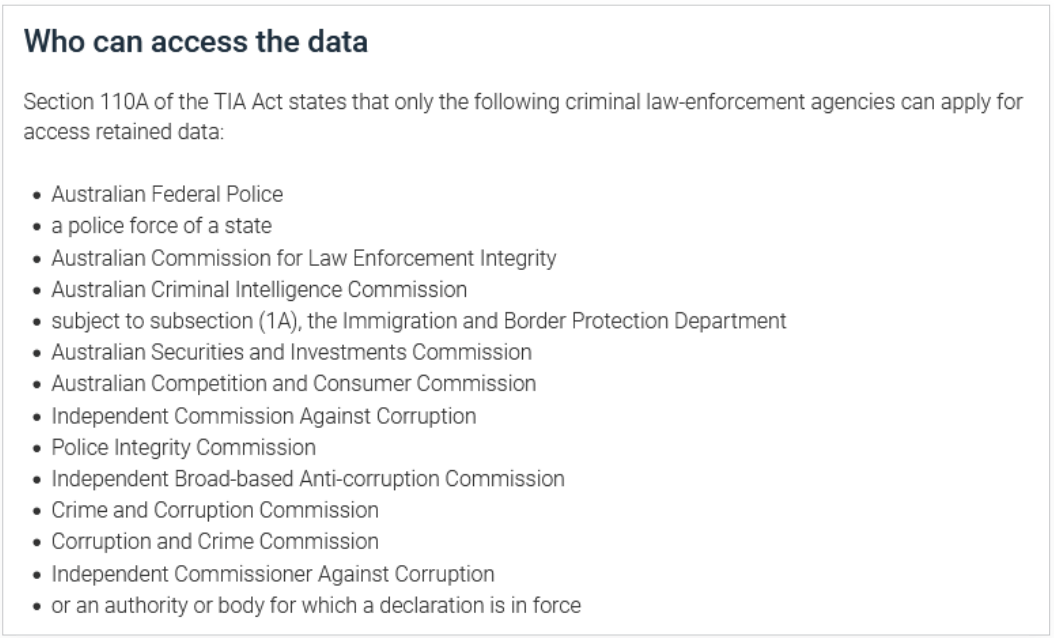


Figure 1 depicting the guide from the Department of Home Affairs on which agencies can access metadata under the scheme. From: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations

4. Access to metadata by these agencies **does not require a judicially authorised warrant**. Unlike many other liberal democracies that require law enforcement agencies to obtain a judicially authorised warrant based on reasonable suspicion to access telecommunications data (for example within the United States, see Churches and Zalnieriute 2020), the **Data Retention Act** permits warrantless access. Law enforcement agencies need only to make a request for data to the relevant ISP. Access to the data "occurs covertly, which means the person to whom the data belongs is not aware of the access and cannot make a complaint if they think the action was unwarranted or unlawful" (Commonwealth Ombudsman, 2021: 5). Therefore, targets of metadata inquiries are unaware that they are being monitored.

5. In response to widespread criticism regarding the implications of the mandatory metadata scheme for journalists the law as passed contained a late-stage inclusion regarding **Journalist Information Warrants (JIW)**. In principle, the JIWs recognise the potential impacts on journalistic practices and in theory provide extra protections for journalists. The law outlines that an authorisation to access the metadata of "a person who is working in a professional capacity as a journalist" or against an individual whom the applicant "knows or reasonably believes to be a source" is not to be granted per the usual procedure. Rather, a JIW is to be pursued instead (see Division 4C of the Act).

A JIW can be granted to law enforcement agencies following approval provided by an "issuing authority" who is a judge appointed by the Attorney-General (see Subdivision C, 180Q of the Act). In granting the warrant the Judge must consider whether the "public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source" (180T 2(b) of the Act). ASIO are permitted a unique line of access to JIWs which can be granted by the Attorney-General following a request from the Director-General of Security (who can also grant a JIW themselves under "emergency" circumstances). Public Interest Advocates (PIA) appointed by the Prime Minister can make "submissions" to the Attorney-General about the conditions of JIWs related to ASIO matters. Journalists are not notified if a JIW has been granted access to their metadata.

At the time the legislation was introduced it was noted that JIWs are easily side-stepped and "if the AFP wants to find out who leaked a government document, it can simply get the call data for all the public servants in the originating department without a warrant and check who called a journalist, rather than wasting time going through a warrant process" (Keane 2015). While the JIWs were introduced to appease concerns about the impact of metadata surveillance on journalism, experience has shown that journalists' metadata has been obtained without a warrant (or without a valid authorised warrant) by Western Australia Police and the AFP (Karp and Taylor 2019). Furthermore, there are questions about who counts as a 'journalist' under the definition provided in the Act. The wording of the legislation refers to "a person who is working in a professional capacity as a journalist" (Division 4C Subdivision A 180G (1)), and it is not clear if this extends to freelancers, or emerging 'citizen/digital journalists.'

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) conducted a review of the **Data Retention Act** and published its findings in October 2020 (PJCIS 2020a). The PJCIS recommended more detailed reporting requirements, improved oversight, tighter conditions on who can be an "authorising officer", and greater clarity around what is considered the "content or substance of a communication" (see PJCIS 2020a: xii–xxi). The introduction of warrants was not recommended.

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) (Assistance and Access Act)

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* was passed in late 2018 and became colloquially referred to as the 'anti-encryption law', the 'decryption law', TOLA, AA Act or **Assistance and Access Act** (see Wilson 2021; Kantor 2019). The motivation behind the law was articulated by (then) Attorney-General George Brandis as creating powers "sufficiently strong to require companies, if need be, to assist in response to a warrant to assist law enforcement or intelligence to decrypt a communication" (cited in Wroe 2017). The law has implications for "designated communication provider(s)" (including but not limited to technology companies) who operate in Australia or with any Australian users and can legally compel 'industry assistance' in the form of either a 'technical assistance request' (TARs), 'technical assistance notices' (TANs), and 'technical capability notices' (TCNs).

While not specifically pertaining to journalists, the **Assistance and Access Act** provides Australian law enforcement agencies with powers to compel assistance from 'designated communications providers' to provide assistance to access to data they have (including any decryption capabilities); to use any capabilities available to 'designated communications providers' against targets of law enforcement; and to 'develop' new 'capabilities' to facilitate access to data. This later aspect triggered concerns the government could introduce a 'backdoor'

or 'systemic weakness' into encrypted forms of communication (Remeikis 2018). As a result, the Government included limits that any "designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability" (Division 7 317ZG of the Act). There is still ongoing confusion about the definition of a "systemic weakness or systemic vulnerability" with the *Independent National Security Legislation Monitor* (2020) recommending clarity to ensure 'designated communications providers' are not requested to introduce capabilities that would amount to 'systemic weaknesses.'

From the perspective of journalists, the **Assistance and Access Act** has several concerning elements:

1. It could be used to weaken the privacy standards of a communication platform. If Australian law enforcement has jurisdictional access to a particular 'designated communication provider', it can compel (with fines for non-compliance) that company into providing assistance. Australian law enforcement may be capable of compromising communication platforms such as WhatsApp, creating risks for confidential communication between sources and journalists that may occur on such platforms. Journalists should therefore consider which platforms and communication channels they use and whether the source code of the encrypted application is open access and can be subject to peer-review (e.g., Signal).

2. 'Designated communications providers' issued with TARs, TANs, and TCNs, **are under strict secrecy not to disclose information or details about any of the assistance provided to Australian law enforcement** with threat of imprisonment for unauthorised disclosure (see Division 6 317ZF of the Act). Therefore, these powers will be exercised in complete secrecy. 'Designated communications providers' can only disclose aggregate data on how many TANs, TCNs, or TARs actioned over a period of 6 months.

The Independent National Security Legislation Monitor (INSLM) is tasked with reviewing the "operation, effectiveness and implications" of the **Assistance and Access Act** powers (Act: p.6) and produced a review in June 2020 (INSLM 2020). It concluded that the new powers available to law enforcement are "necessary" (ibid: 24) and recommended clarification on the definition of "systemic weakness", including the need for the Administrative Appeals Tribunal (AAT) to rule on such a definition, in addition to other amendments about who can issue TANs and TCNs. Annual reports provided by Home Affairs indicate that TARs are more commonly used than TANs or TCNs, with 11 TARs issued in 2019–20 while zero TANs or TCNs were issued (Department of Home Affairs 2020: 78).

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) ('Identify and Disrupt Act')

The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* was passed in August 2021 and gives significant new government hacking powers to the AFP and ACIC and assistance may be provided by the ASD (see The Parliament of The Commonwealth of Australia, 2020). The **Identify and Disrupt Act** creates three new warrants: 'data disruption warrants', 'network activity warrants' and 'account takeover warrants.' In combination, the warrants provide the AFP and ACIC with a wide range of capabilities including the power to 'disrupt data' which includes "adding, copying, deleting or altering" data within any computer or data-in-transit that they can intercept and are authorised to access (Schedule 1 27KE). 'Network activity warrants' provides warrants against "electronically linked" groups (broadly defined) and permits monitoring of a range of computers or devices (even when it is not known who is using devices or the devices' physical location) (Schedule 2 27KP). Finally, 'account

takeover warrants' allow the AFP or ACIC to "take control of one or more online accounts" (Schedule 3 Division 1 3ZZUJ) (in conjunction with other warrants and authorisations).

The **Identify and Disrupt Act** has several concerning elements for journalists:

1. The definition of "network" and "electronically linked" is broad and allows for surveillance that could capture journalists or their sources. While the relevant Judge or Administrative Appeals Tribunal member is required to consider whether a journalist is likely to be impacted by the warrants and weigh both the "public interest in protecting the confidentiality of the identity of the journalist's source" and the "public interest in facilitating the exchange of information between journalists and members of the public" (see Schedule 1 27KC (ce) and elsewhere), there is no express prohibition on the exercise of the powers against journalists and their sources (even when this is a foreseeable or possible outcome) nor requirements for law enforcement to obtain a Journalist Information Warrant as per the data retention scheme. This is further compounded by the power to hack devices when the identity of the device-user is unknown, thus allowing 'blind hacks' that potentially capture journalistic activity.

2. The threshold of seriousness is low. While political rhetoric focused on issues of serious organised crime, terrorism, and child sexual abuse, the legislation as passed permits hacking activities for activities "against the security of the Commonwealth", "against the proper administration of Government", and any conduct that "has the potential" to cause harm, damage or danger to a "person", the "community", or "critical infrastructure" (see Schedule 1 27KC (3) and elsewhere). It should also be noted that approval of the warrants is not limited to these offences and can rest on the discretion of the relevant Judge or member of the Administrative Appeals Tribunal to approve for a wider set of conduct.

The **Identify and Disrupt Act** introduces a new suite of considerations for journalists. This is pertinent to instances when these agencies may be the target of a journalistic investigation, or when the journalist suspects their source may be of interest to the AFP or ACIC.

Telecommunications Legislation Amendment (International Production Orders) Act 2021 (Cth) ('IPO Act')

The United States and Australia have entered into a bilateral agreement to share data under the *Clarifying Overseas Use of Data (CLOUD) Act* (US) (see Agreement Between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, 2021), and the passage of the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* (Cth) supports this in the Australian domestic legal framework. The **International Production Orders Act** allows for Australian law enforcement agencies access to telecommunications data stored in foreign jurisdictions (i.e., directly from US based designated communications providers) and for foreign law enforcement agencies to reciprocally access data stored in Australia. This means that US authorities can access Australians' information directly from US based designated communications providers and includes providers of messaging applications, video calls and cloud storage services.

In practice, this has potential implications for Australian journalists as Australian law enforcement and intelligence agencies may be able to access their information directly from US based companies, for example, if they were to store information in US based cloud services, or communicate with sources over messaging

applications or video calls operated by US based organisations. In its submission to the PJCIS (PJCIS, 2021, p. 30, emphasis added), the Law Council of Australia, noted that:

> "It seems to us that there are no legal safeguards in the bill that would prohibit Australia from giving domestic legal effect to an agreement that could be used to disclose information that could in turn be used to inculpate a person in foreign death penalty proceedings; to prosecute a child as an adult; to prosecute a person for a political offence that, in substance, targets peaceful dissent, advocacy or discussion' to violate rights to freedom of expression, *such as targeting a journalist's source or telling a journalists to disclose their sources*; and to prejudice a person's right to a fair hearing by targeting and using information that's subject to client legal privilege".

In its advisory report on the *Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020* the PJCIS (2021, p. xvii) recommended the Bill be:

> "amended to implement the recommendations set out in the Committee's [PJCIS'] report of its *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press*, including recommendation 2 (i.e. that the current role of the Public Interest Advocate, as provided for under the *Telecommunications (Interception and Access) Act 1979* be amended in line with the terms of that recommendation and expanded to apply to applications for international production orders.

Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press

In response to the raids on the ABC and other actions against journalists in Australia in July 2019 the Attorney-General referred the PJCIS (2020b, p. xi) to conduct an inquiry and report back to both Houses of Parliament on, *inter alia*, "the experiences of journalists and media organisations that have, or could become, subject to the powers of law enforcement or intelligence agencies performing their functions, and the impact of the exercise of those powers on journalists' work, including informing the public" and "the reasons for which journalists and media organisations have, or could become, subject to those powers in the performance of the functions of law enforcement or intelligence agencies."

The PJCIS reported its findings and recommendations to Government in August 2020 which contained 16 Recommendations (see PJCIS 2020b). These recommendations included the expansion of the role of the Public Interest Advocate (PIA) and the Journalist Information Warrant (JIW) and recommended that warrant provisions to access telecommunications data be amended to include "mandatory consideration of warrant applications by Public Interest Advocates (PIAs) to cover all overt and covert warrants that relate to a person working in a professional capacity as a journalist or a media organisation, where the warrant is related to the investigation of an unauthorised disclosure of government information" (Recommendation 2); additional record-keeping by and reporting about the PIA (Recommendations 3;4;5); and that "the Australian Government give consideration to the formulation of a mechanism to allow for journalists and media organisations, in the act of public interest journalism, to consult with the originating agency of national security classified information without the threat of investigation or prosecution" (Recommendation 8).

Recent adversarial actions against journalists in Australia

The introduction of new electronic surveillance capabilities as described above has coincided with adversarial action against Australian journalism. The most significant moment was the raid of the Sydney offices of the national broadcaster the ABC by the AFP on June 5th 2019. Holding a warrant with the ability to "search", "alter" or "delete" documents founds in the ABC computer systems, six AFP personnel scanned emails and documents relating to reporting of allegations of Australian war crimes (Lyons 2019; Knowles et al 2019). In the 24 hours prior to raiding the ABC, the AFP also executed a warrant against News Corp journalist Annika Smethurst for reporting on new surveillance powers for the Australian Signal Directorate (ASD) (ABC 2019). Also on the same day, another journalist, 2GB's Ben Fordham, was contacted by a representative of the Department of Home Affairs and notified of an investigation into his source on a story on asylum seekers, leading Fordham to believe he could potentially be targeted by AFP warrants (see Sky News 2019).

The events of the 4th and 5th of June 2019 demonstrated the posture of the AFP and Department of Home Affairs towards journalism, journalists, leaks and sources. As articulated by the head of ABC investigative journalism, John Lyons, the events marked a "new climate in which journalists and their sources of information" are targeted with "the sort of treatment previously reserved for criminals and terrorists" (Lyons 2019).

The raids were a signifier for many of our participants that they need to reassess their information security practices. Several other recent events also raised journalist's alertness including the cases of Bernard Collaery, David McBride, and Richard Boyle. Collaery is an Australian barrister who was facing trial at the time of the project for receipt of classified information from Witness K concerning ASIS surveillance of East Timor officials during negotiations about undersea oil and gas reserves (see Mann & Daly, 2019); McBride is a former ADF lawyer accused of leaking information on war crimes committed by Australian forces to the ABC; and Boyle is a former public servant in the Australian Taxation Office (ATO) who spoke with the ABC and Nine about ATO action against small business owners and is currently facing prosecution. The cases demonstrate government hostility towards whistle-blowers and an aggressive response to disclosures made in the public interest (note: the charges against Collaery were dropped by the new Labor government's Attorney General in July 2022).

Several other events are contextually relevant for the fieldwork period for this research (between May and November 2021). The former Attorney-General, Christian Porter, launched high-profile defamation proceedings against ABC journalist Louise Milligan (but then dropped the action). 'Citizen Journalist' and YouTuber Jordan Shanks (aka 'Friendlyjordies') was pursued for defamation by (then) Deputy Premier of New South Wales John Barilaro, and his producer Kristo Langker was arrested and accused of 'stalking' Barilaro. Notably, Shanks and Langker were targeted by the New South Wales' 'Fixated Persons Unit' a taskforce typically reserved for violent extremists (see Knaus 2021). Further, in the context of protests around COVID-related restrictions, Victoria Police arrested a Herald Sun journalist and photographer (Paynter 2021) and they detained 'citizen journalist' Avi Yemini in 2020 while repeatedly confronting him at several protests (see Loomes 2021; Rebel News 2021). These events provided the backdrop of this research and informs the context under which our interviews took place.

Methods: What did we do?

The findings in this report are based on original research conducted by the authors between May and November 2021. The primary form of empirical investigation was in-depth interviews with 19 journalists and 2 media lawyers who represent or advise media organisations and are based in Australia. Journalists from multiple major Australian news organisations participated, and the sample mostly consisted of journalists who had 'investigative' roles and who were likely to be subject to attention and scrutiny by law enforcement or public authorities in Australia. Former journalists and freelancers also participated, in addition to journalists who had reported on surveillance and were familiar with Australian surveillance law.

All interviews were conducted under an agreement of complete participant anonymity. We did not record any names and therefore no individuals or organisations are named in the reporting of the findings and all quotes are unattributed. Interviews were not recorded to protect sensitive information, and instead, detailed notes were taken of the interview topics by our Research Assistant. Interviews lasted approximately an hour.

The goal of the interviews was to gauge knowledge, awareness, and confidence with information security, source protection, and surveillance powers in Australia. Individuals were asked to gauge their own abilities and concern around communicating securely with sources and handling data such as leaked documents. They reported the level of organisational support received and associated education or training. Participants were also asked to provide their views on how the surveillance laws have impacted upon journalism in Australia. Participants were also asked their views on how to improve the information security practices of journalists. Media lawyers who represent journalists were asked a similar set of questions with stronger focus on legal implications and how the digital age has impacted the advice they provide to their journalist clients and media organisations.

Part B: Journalist's Surveillance Awareness and Information Security Preparedness

One aim of this research was to investigate Australian journalists' awareness and preparedness around electronic surveillance and threats to information security. There was variation between journalists in knowledge, understanding, and practical skills in protecting their information security. Similarly, there was variation between media organisations in institutional efforts to train, inform, and support journalists. Several media organisations offered no training or support, while some organisations offered occasional seminars or information sessions. Ultimately, for most journalists working in Australia, responsibility for developing skills and understanding around their digital threat profile and the steps to manage their information security was an individual responsibility. Except for peer support in some organisations, information security was largely left in the hands of individual journalists.

Understanding that information security is devolved to individuals is key to understanding journalists' preparedness, and how to improve journalistic practice in a digital era. This chapter details the views of journalists (and two media lawyers) in terms of self-assessment of their skills. The chapter outlines how the AFP raids on the ABC were a trigger for enhanced awareness of potential state surveillance. The chapter concludes by considering ways for improving journalist understanding of surveillance and information security skills.

a) Journalist knowledge of state surveillance and information security skills

There were a small set of journalists across several organisations who were recognised by their peers for having considerable insight, experience, and advanced levels of knowledge about electronic surveillance and information security. These individuals played an informal role within their organisations as a 'go to' person for advice or had led seminars, workshops, or events either within their organisation or externally. These individuals could speak knowledgeably about TOR, privacy-focused distributions of Linux such as Tails, and had technical understanding of how an encrypted communications applications such as Signal operates (and how to evaluate trust in a service or application; in what circumstances it is useful; and what sort of risks still remain). These individuals were instigators of introducing mechanisms such as SecureDrop into their organisation, and on one occasion a journalist outlined how they operated their own .onion 'drop point' for sharing documents with a source.

The journalists with the highest levels of awareness and understanding generally did not have formal training or qualifications in information technology and they educated themselves to securely perform journalism in a digital age. The small of number of journalists identified by their peers as holding knowledge were still limited to what they could self-teach (and this was competing with several time and resource factors). Likewise, the technical

ecosystem is constantly evolving with new surveillance powers, threats and vulnerabilities, and journalists have limited capacity to keep-up with ongoing developments. Take for example this reflection:

> If Signal was compromised — I would only know about it because of a big story, and the lag between its compromise and the revealing of that compromise just means you are hammered in the interim. (Journalist M)

Trying to 'keep up' with information security developments is a relentless task that requires time and resources:

> It is so hard to keep up — it is so complicated — you need an update every three months. You need someone who is booking in a meeting with you to go through social media and the apps on your phone: what you have saved in places, what needs to be deleted and destroyed; that is the only way you can be sure. (Journalist F)

This led to "very low confidence" (Journalist F) that journalists were protected. As an example of how information security concerns can shift and require new risk calculations, during fieldwork the encrypted email client Protonmail had provided the IP address of a climate activist in response to a warrant sought by Europol and French Police (see Brandom 2021). This illustrates how trust in and reliance on certain tools fluctuates, adding to the workload of journalists. Even the most dedicated and skilled journalists cannot be realistically expected to keep up to date with all information security developments, thus creating an ongoing challenge to reassess and re-evaluate information security strategies.

Compared to the technically knowledgeable journalists described above, most journalists admit that they do not have the necessary understanding of electronic surveillance and information security or have only recently considered information security practices (in response to the AFP raids on the ABC). These journalists may require additional professional development to be able to competently manage surveillance threats. Some suggested they did not have enough confidence in their own skills that if a source wanted "full assurance of being protected" they "would not be able to guarantee this" (Journalist J). Another identified that to keep up to date with matters of information security you needed to be "highly motivated to be highly secure" (Journalist D), and that they did not have that level of motivation and instead made sure they are not doing "stupid things". Others conceded that when it came to information security they did not think about it "enough" (Journalist Q), and others were "learning on the job but could know more" (Journalist I).

Some journalists in this group had recently started using encrypted email clients such as ProtonMail. For example, Journalist J who suggested he did not "think much about [information security] beforehand". Likewise, Journalist P also suggested that information security was something they "never really considered it strongly" and that "everyone in the world of journalism wasn't really thinking about it", but that this had changed with widespread migration to encrypted messaging apps. Journalist A suggested they are using Signal a lot more and Journalist B suggested they have now migrated most online communication to "Protonmail or Signal" because of information security concerns. While the migration to platforms such as Signal and Protonmail that have good information security credentials is a positive development, as suggested by Journalist U most journalists do not "really (go) beyond using Signal." For most journalists, their information security awareness consists of reliance on tools such as Signal and Protonmail, but not dedicating time to understand information security beyond that.

b) The impact of the AFP raids

The June 2019 AFP raids on the ABC and the home of NewsCorp Journalist Annika Smethurst brought information security into sharp focus for journalists. Journalist P described it as a "holy shit" moment that put journalists and media organisations on "high alert" about surveillance. Journalist C outlined how the raid signalled how "in the last 10 years or so things have changed" and suggested that "the AFP walking into journalist's offices and home was unthinkable 15 years ago". Journalist C argued that it has specifically driven "more of an institutional awareness across most of the big media companies across Australia" and lead to Signal and Protonmail becoming more "en vogue". Journalist B outlined how the raids had a "profound impact" in influencing the way they operated and made them realise "how hard it is to make sure everything is safe when trying to protect someone". Likewise Journalist I described it as a "wake up call for some people"; Journalist J said that they think more about information security after the raids; and journalist F described how there is a new acceptance that "anything can be surveilled" where previously "there was a certain expectation — pre the raids — that within certain boundaries, the enforcement agencies and police could not access journalistic information that was part of content making".

The AFP raids raised the 'alert' level around electronic surveillance in Australia. As outlined above, this was viewed as "entering a different era" where there is an "entitlement to go after journalists" (Lawyer A), marking a shift from previous understandings that journalism was to be respected with a 'hands-off' approach. It forced several media organisations to give more attention to information security. Journalist N described how some media organisations now have "protocols" in the event of a raid and are pro-actively thinking about their exposure level if the AFP (or any other agency) were to seek access to the devices of journalists or the media organisations in which they work. Individual journalists are giving more thought to information security and migrating to encrypted communication platforms, while thinking carefully about communication with sources and the storage of information over the longer-term. The AFP raids had the consequence of raising information security concerns.

c) Lack of institutional support and self-reliance of journalists

While the AFP raids prompted more concern for information security within media organisations, the journalists that we spoke to reflected that they received little institutional support with limited or no training, policies, or support structures. As suggested by one journalist who works across multiple outlets "media organisations cut you loose basically" (Journalist T) with pressure on journalists to undertake 'DIY' training. When asked whether they had received any support or advice from their organisation one journalist reflected:

> Nothing was explicit. This is something you learn but nobody explicitly tells you to do this. You are not trained in this as a journalist.
> (Journalist K)

Some journalists reflected that some media organisations offered dedicated seminars or information security classes which were well-received, but sporadic and unlikely to cover everything required in one session. Training across media organisations was described as "inadequate" (Journalist D) and for most, the training is "very much 'on the job'" (Journalist N). Individuals come to rely on peers and will "discuss information security amongst themselves" (Journalist P). One of the most knowledgeable journalists on information security stated that it is "normal for journalists" to not expect institutional support and "as a journalist if you want to learn about

something then you do it yourself" (Journalist C). This journalist described how their editors, until recently, "did not get the urgency and secrecy about why in person meetings would still be necessary". Likewise, another journalist suggested "you are mad if you want a large organisation to update policy" or provide directions and "should never have faith in organisations to update in time for the real-world challenges" which means you must "stay ahead and rely on yourself" (Journalist M).

Journalists understand that "it is up to the individual journalist to make sure they are secure" (Journalist A) with a lot of "figuring it out for yourself and informal networking" (Journalist E). Media organisations are "too busy trying to get stories to air" to spend time ensuring staff have information security preparedness (Journalist K). Relying on journalists to self- educate presents risks. An example is how The Intercept accidently informed the FBI that Reality Winner leaked NSA documents (Stuart 2021). Media organisations could do more to support journalists and educate them on information security strategies.

Improving journalist cyber-security awareness and preparedness in Australia

We asked journalists 'what could be done to improve the general information security awareness and practices of journalists?' Many emphasised that media organisations are financially constrained and argued that media organisations could do more training to support staff. Journalist P, for example, argued that there should be "formalised training" and "organisational support" for journalists to be "safe and secure", but this needs to be balanced against the reality that "putting aside a day in mainstream media organisations … is going to be problematic because they just scrape by". There is limited time to commit resources outside of delivering stories in a 24-hour news cycle.

Many journalists emphasised how media organisations "need to do more to invest in training for journalists for cyber-security" and that "this is done for defamation, but the same approach should be done for information security risks" (Journalist I). Journalist D suggested that "security is probably too far down the list of considerations". Journalists need "more information and support" (Journalist G), and the media organisations should be providing training on a regular basis. Journalist H stated that "more regular meetings on secure investigation are also needed" and at a rate of perhaps "quarterly to top up training for cyber security" and keep an ongoing discussion around "what device people use to do investigative reporting". The "proprietors, big companies and the leadership of the news organisations of the big companies need to do more" (Journalist K), but it was recognised that "not all staff need this" and investment in training should be targeted, for instance journalists who "wish to do serious national security work" (Journalist G) or those that receive unauthorised disclosures. This is an important investment:

> It is something that journalist organisations need to invest more in. Ultimately it is going to protect the way the organisation works and the free-flow of information that journalists rely on.
> (Journalist I)

One journalist emphasised that "if it is widely known that journalists are good at this, then more sources might come forward" (Journalist J) which relates to how journalists inform and coach sources in information security. A problem is that "they get a lot of overzealous sources" that do not go through the "secure channels" and so it is an important task to be "educating sources of when they have to be aware of their interaction with you" (Journalist F). Others outlined how "sometimes sources are not aware of the digital trail they are leaving, and this

makes it tricky to communicate with them" (Journalist I). Approaches by sources have been "unsophisticated … which can blow the story up before it starts" (Journalist Q). Sources have "varying degrees of education" on information security, with some "confident approaching with encrypted apps" while on other occasions "you sometimes have to gently guide sources to Protonmail and Signal" (Journalist P).

Some organisations are pro-actively directing and guiding sources to securely approach journalists. The public-facing webpages of multiple media organisations in Australia (i.e., the ABC, The Age, The Guardian Australia, and Crikey) show they have already implemented 'SecureDrop' to allow for more secure sharing of documents. Some organisations like 9News were requesting 'tip-offs' via a generic email address or their own 'wetransfer' service (note: based on observations in 2021). Some news outlets are attempting to inform sources of more secure ways of approaching journalists, but this remains patchy with several major newsrooms continuing to provide basic contact information and encouraging easily compromised modes of communication.

Most journalists were promoting their Protonmail email address or Signal contact information on their public-facing profiles. However, it should always be noted that while tools such as SecureDrop, Protonmail, or Signal have some security advantages, the threat environment is constantly changing and journalists need quality information about how to utilise such tools securely (i.e., these tools only protect data-in-transit and any endpoint compromise will be disastrous for journalists and their sources or the use of insecure and recycled passwords could readily compromise an account). Over the long-term media organisations need to respond to new surveillance capabilities and powers, and keep journalists informed of evolving 'best practice'.

Media organisations may improve the information security of journalists by investing in training on surveillance powers, and defensive practices. They could also consider building internal and external advice networks and expertise could be harnessed by knowledge-mobilisation and networking within organisations through recognised mentors or working groups who accumulate and disseminate knowledge of information security 'best practice'. There are many freely available resources and professional networks that could be harnessed to support journalists in Australia. For example, Posetti, Dreyfus and Colvin (2019) developed "The Pergugia Principles for Journalists Working with Whistle-blowers in the Digital Age", and organisations such as the Freedom of the Press Foundation are developing secure communication tools including SecureDrop. The ICIJ recommended tools to protect sources (Woodman 2018), and guides for journalists are available including via the Global Investigative Journalism Network (GIJN 2022).

Part C: Impacts of Surveillance Law on Journalism and Reform Recommendations

This research also explored the potential impacts of the **Data Retention Act**, the **Assistance and Access Act**, the **International Production Orders Act**, and the **Identify and Disrupt Act** on Australian journalism. Journalists have a general awareness of these surveillance powers, however, did not always understand the specifics (except for a few journalists that had reported actively on the surveillance laws). Journalists had a good understanding of the metadata retention scheme and understood the state surveillance powers were increasing and greater information security precautions were required. Journalists did not identify direct consequences of specific laws, rather felt the state's aggressive stance towards journalism in Australia had escalated and that surveillance was a central part of this 'climate'. This intersected with broader concerns about attitudes to whistle-blowers, unauthorised public disclosures, and prominent defamation cases. There was a general cynicism that 'everything is being surveilled' and while many journalists emphasised that this would not deter them from covering stories or pursuing investigative inquiries, many conceded that they had lost sources, and had lost confidence to offer assurances for source protection. A notable theme was that journalists were far more likely to be concerned about the surveillance of their sources and whistle-blowers than themselves.

a) Cynicism and surveillance powers: "If government wants it, they can get it" (Journalist C)

Journalists reflected that law enforcement and intelligence agencies had ample powers to conduct surveillance of journalists and their sources.

> … there does not seem to be a limit in the powers granted to law enforcement. They ask for something and generally they get it.
> (Journalist D)

For many journalists the assumption was that "if someone really wants to get to your source – there will be a way for them to do that" and that "anyone can access almost anything" (Journalist B). Others suggested that even when using 'secure' modes of communication that you should "operate under the rule that anything in writing can be discovered – whatever the software is" (Journalist G). The prevailing sentiment was that "if the government really wants to chase after you, you should never bet against their capacity to find out the information" (Journalist Q) and "the media probably won't win the battle against the government on surveillance" (Journalist Q). The introduction of enhanced surveillance powers in Australia created a sense that digital communication was already compromised or could be readily compromised.

b) Losing sources

One impact of the enhanced surveillance powers was the loss of sources. One journalist articulated how new surveillance powers meant that they are "much more cautious about talking to sources" and that they had a situation where they had to "drop contact" with a source as they were certain "the source was watched" (Journalist Q). Likewise, another journalist described how some sources make mistakes when communicating via "overt means" (i.e., via insecure modes of communication) and they have been unable to offer source protection (Journalist M). One journalist described an approach that an anonymous source had made by sending them a USB drive containing leaked documents, and when the journalist checked the document properties in Word they could identify the creator of the documents. Other journalists have had sources withdraw following "conversations about electronic security measures" when the source may not have taken steps to protect their identify (Journalist N). The surveillance powers in Australia are complicating the journalist–source relationship and in some cases, this has meant journalists lose sources. In some circumstances "sources who contact journalists do seem to want to go through with the process." (Journalist N). However, in general, "it is more difficult to protect sources and whistle-blowers these days" (Journalist J).

c) Priority concern for whistle-blowers

Journalists remarked that new surveillance powers make whistle-blowers "less likely to come forward" (Journalist H). Journalist A commented that while you cannot "pinpoint a specific law" and its impact upon sources, the enhanced surveillance powers impacts on "how willing people are to come forward and talk to journalists" and that "it is harder to get people to provide information because the risk is so great". Notably, journalists were less concerned for themselves and were more concerned about how whistle-blowers are potentially being surveilled. A journalist outlined that although the surveillance laws are a "pain" they do not "impact editorial decisions to cover things", and the main negative impact is the limited "ability for people to come forward and tell stories" (Journalist F). Others suggested that the surveillance powers are unlikely to "change the way journalists operate day-to-day but the greater danger is the message it sends people who are contemplating using the institution of journalism to get information out" (Journalist I).

One journalist commented that "all journalists like to think of themselves as martyrs" and there is less concern for themselves and more concern for their sources (Journalist P). Journalist Q outlined how "metadata retention" has made first contact with sources "fraught" and that "even if the contact was very little, there would still be risk". Overall, for some journalists the impact of increased surveillance powers is clear and that "there is a massive chilling effect on stories" (Journalist G) and is felt acutely by sources who "are not coming forward as they once did" (Journalist M). One journalist summed it up as the laws were to "fuck over whistle-blowers" (Journalist K) and a media lawyer stated that "these laws seem to be purely to punish the whistle-blowers" (Lawyer B).

d) Surveillance powers as part of the climate against journalism

Enhanced surveillance powers were one dimension of a climate of hostility towards a free press, whistle-blowers, and state transparency in Australia. The AFP raids signalled an escalation in hostility towards journalists and coincided with the prosecution of whistle-blowers including David McBride, and the prosecution of ATO

whistle-blower Richard Boyle. Several journalists suggested that there was a developing "culture of secrecy" (Journalist M) and that "even basic information about the way governance is run are being silenced" (Journalist F). The willingness of public authorities to pursue and prosecute whistle-blowers and sources increasing with "really high profile punishment of whistle-blowers in recent years" (Journalist H), and this is "all about intimidation" (Journalist K).

Australia's "hyper-legislative" approach in response to terrorism, which includes 92 anti-terrorism laws introduced since 2001 (see Roach, 2011; Ananian-Welsh and Hardy 2021), was identified as contributing to the opacity of public institutions which prevents journalists "from doing their jobs" and having "ramifications here for journalists to scrutinise government" (Lawyer B). Likewise, defamation law in Australia was identified as "curtailing" the coverage of stories (Journalist H) and journalists are worried about how defamation interacts with information security, particularly the potential revealing of "source material in a defamation proceeding" (Journalist K).

Surveillance powers are experienced in conjunction with other hostility towards public disclosures, whistle-blowing, and a free press. Overall, most journalists expressed that while there were no major editorial impacts (i.e., they would not avoid covering a story because of the potential for state surveillance), there was a sense that "everyone is being a lot more careful" (Journalist P) with "chills in the gathering of information" (Journalist Q). As stated by Journalist P:

> Interviewer: *Do these laws have editorial impacts on the stories you do?*
>
> Journalist P: *No. Not in the slightest but there are changes in the way you do stories … When you realise what law enforcement can do, you must be more careful.*

Protecting journalism with reform

This final section explores journalists views on surveillance law reform and offers some preliminary recommendations. Journalists pointed to a need to improve press freedom which has also been suggested by organisations such as the MEAA, the 'Right to Know' campaign, and Blueprint for Free Speech, among other advocacy organisations.

One journalist suggested to repeal all the surveillance laws and undertake widespread reform, which notably, is currently underway following the Richardson Review:

> Interviewer: *Are there specific ways the laws could be changed?*
>
> Journalist K: *No. Just get rid of them … We don't need these laws, we didn't need them in the first place. Why we passed something like this is a joke.*

Another journalist called for consideration of the necessity of the surveillance powers:

> *Taking a step back and seeing if we need this electronic surveillance is important too — is it necessary? And taking into account the potential impact of journalism? And not just using the excuse of 'terrorism' all the time.* (Journalist J)

Not all journalists were opposed to surveillance powers, and some acknowledged the "need for metadata retention" (Journalist M) or could see how individuals suspected of committing criminal offences are using digital communications and a "sensible balance" between "journalist and source-rights with public safety" was required (Journalist B).

One reform possibility that several journalists mentioned was the requirement for a warrant to access metadata in any circumstance (and not just the requirement for a journalist information warrant, JIW). Most journalists were critical of JIWs, and a possible solution was to require a warrant for *all* instances where access to retained metadata was sought. JIWs were considered "not that meaningful a protection at the end of the day" (Journalist H), that "it is not enough" (Lawyer A), with no "trust in it at all" (Journalist Q), and there was "little faith in procedures" around JIWs (Journalist R), with one journalist (J) suggesting that they "don't know anyone who feels like it helps". One journalist (S) considered that "it's a guise – it doesn't actually protect journalists" and the lack of transparency around JIWs was a major concern: "a safeguard is only a safeguard if it is transparent" (Journalist N).

The protection provided by the JIWs was considered so weak that "there is always a truck you drive around these [protections such as JIWs]" (Journalist T). The most important reform to protect journalists, their sources, and the public more broadly is to require judicially authorised warrants for access to retained metadata: "warrants should be required for everyone. These should be required in court and required universally" (Journalist L). Journalists consistently remarked that law enforcement should need to "get a warrant for everyone" (Journalist A) and there should be "some sort of process where they (law enforcement) go before a judge" (Journalist B). The protections provided to journalists should "be given to everybody" particularly where there are issues in relation to "how you define what journalism is and who gets an exemption" (Journalist D).

The issue of requiring a judicially authorised warrant to access metadata has been raised by several interested organisations including the Law Council of Australia and the Australian Human Rights Commission, among others (see e.g., Duckett 2019, AHRC 2019). A requirement for judicially authorised warrants to access metadata would provide greater protections for journalists, whistle-blowers and sources and is vital for a free press (in addition to protecting the privacy of all Australian citizens and residents).

Journalists proposed a range of other recommendations for reform including restrictions on the **Identify and Disrupt Act** powers to the most serious offences (Journalist A), which would be consistent with the rationale supporting the introduction of the powers. As outlined in PART A above, the threshold for the seriousness of offence that can trigger the use of invasive 'data disruption warrants', 'network activity warrants' and 'account takeover warrants' includes any conduct that "has the potential" to cause harm, damage or danger to a "person", the "community", or "critical infrastructure" (see Schedule 1 27KC (3)). Journalist A argued that "they need to narrow the range of offences that they want it to be appropriate for" and articulate limits to the most serious types of offending. Murray and Mann (2020) have also argued that the law should specify "an exhaustive list of specific offences" for which the powers can be used.

Other journalists suggested recommendations including the introduction of an Australian Bill or Charter of Rights providing enforceable human rights protections against surveillance (Journalist C). Others called for greater protections for whistle-blowers, stronger media protections such as the introduction of a Media Freedom Act (Lawyer B) (see Greste and Murray 2019), and an improved public interest disclosure scheme (Journalist P). Advocates for enhanced whistle-blower protection have previously outlined detailed policy suggestions (see Brown et al 2019).

Finally, journalists argued that surveillance should be used consistent with the intent and limits as established by law. This is relevant as a wide range of organisations and agencies are accessing metadata including non-law enforcement entities; journalists' metadata has been accessed without the required JIW; that internet service providers are retaining more data than mandated; and the AFP has a "cavalier" attitude to how they manage access to retained metadata (Commonwealth Ombudsman 2021). Journalist A commented that the illegal access to journalists' metadata is not being met with any "punishment" and is likely to continue. Other journalists

called for stronger "auditing" of how surveillance powers are used (Journalist T). Journalists believe that it is important that law enforcement comply with the current surveillance laws with increased transparency and meaningful accountability for breaches.

This research was conducted at a time of significant reform of the legal framework governing telecommunications surveillance in Australia. In early 2018 the Australian Government commissioned a review of the legislative framework governing telecommunications surveillance in Australia which was conducted by Dennis Richardson (a former Director General of ASIO) (see Kirby, 2021). A classified version of Richardson's report was delivered to the Australian Government at the end of 2019 and a declassified version made publicly at the end of 2020 (see Attorney-General's Department, 2020). It made 203 recommendations that centred around the repeal of all existing telecommunications surveillance legislation and the enactment of a consolidated *Electronic Surveillance Act*. In response Richardson's recommendations, the Department of Home Affairs (2021) released a discussion paper about the 'Reform of Australia's Electronic Surveillance Framework' and invited public submissions. The Department of Home Affairs indicated that it will release an exposure draft of the proposed *Electronic Surveillance Bill* in late 2022, with consultation before finalisation in 2023. This wholesale reform of the legal framework governing telecommunications surveillance in Australia represents an important opportunity to advocate for enhanced protections for journalists and their sources, as well as all Australian citizens and residents.

References

ABC (2019) Scott Morrison defends Federal Police raid on journalist Annika Smethurst's Canberra home. *ABC News*. Available online.

African Digital Rights Network (2021) *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*. Available online.

Agreement Between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (2021). Available online.

AHRC (2019) 'Metadata law' review makes key changes. *Australian Human Rights Commission*. Available online.

Amnesty International (2021) *The Pegasus Project: Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*. Available online.

Ananian-Welsh R, Kendall S, & Murray R (2021) Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom. *Melbourne Law Review, 44*(3), 764–811.

Ananian-Welsh R (2020) Smethurst v Commissioner of Police and the Unlawful Seizure of Journalists' Private Information. *Media and Arts Law Review, 24*(1), 60–71.

Ananian-Welsh R (2019) Journalistic confidentiality in an age of data surveillance. *Australian Journalism Review, 41*(2), 225–239.

Ananian-Welsh R and Hardy K (2021) Before 9/11, Australia had no counter-terrorism laws, now we have 92 — but are we safer? *The Conversation*. Available online.

Attorney-General's Department (2020). Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community. Available online.

Brandom R (2021) ProtonMail court order leads to the arrest of French climate activist. *The Verge*. Available online.

Brevini B (2017) Metadata Laws, Journalism and Resistance in Australia. Media and Communication, 5(1), 76–83.

Brown AJ, Lawrence S, Olsen J, Rosemann L, Hall K, Tsahuridu E, Wheeler C, Macauley M, Smith R, and Brough P (2019) *Clean as a whistle: a five step guide to better whistleblowing policy and practice in business and government*. Key findings and actions of Whistling While They Work 2, Brisbane: Griffith University. Available online.

Churches G and Zalnieriute M (2020) A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA. *AusPubLaw*. Available online.

Commonwealth Ombudsman (2017) *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*. Available online.

Commonwealth Ombudsman (2021) *Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020*. Available online.

Crete-Nishihata M, Oliver J, Parsons C, Walker D, Tsui L, and Deibert R (2020). The Information Security Cultures of Journalism. *Digital Journalism* 8(8): 1068–1091

Department of Home Affairs (2021). Reform of Australia's electronic surveillance framework discussion paper. Available online.

Di Salvo P (2021) Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection. *Digital Journalism* 9(4): 443–460

Duckett C (2016) 61 agencies after warrantless access to Australian telecommunications metadata. *ZDNet*. Available online.

Duckett C (2019) Law Council wants warrants and crime threshold for metadata retention scheme. *ZDNet*. Available online.

Eide E and Kunelius R (2018) Whistleblowers and journalistic ideals: Surveillance, Snowden and the meta-coverage of journalism. *Northern Lights: Film & Media Studies Yearbook* 16(1): 75–95

Farrow R (2019) The Black Cube Chronicles: The Private Investigators – How two operatives tasked with surveilling reporters became embroiled in an international plot to suppress sexual-assault allegations against Harvey Weinstein. *The New Yorker*. Available online.

Global Investigative Journalism Network (2022) *Digital Security*. Available online.

Greste P and Murray R (2019) Why Australia needs a Media Freedom Act. *The Political Economy of Communication* 7(2): 105–108.

Henrichsen J R, Betz M, and Lisosky J M. (2015) *Building digital safety for journalism: A survey of selected issues*. UNESCO Publishing.

Henrichsen J R (2020) Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism* 8(3): 328–346

Home Affairs (2021) *Guide on the 'data set' to be collected by ISPs/Telcos*. Available online.

Humphreys S & De Zwart M (2017). Data retention, journalist freedoms and whistleblowers. Media International Australia, 165(1), 103–116.

Independent National Security Legislation Monitor (2020) *Trust but verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*. Available online.

Kantor S (2019) Decryption laws update – what's the latest? *Minter Ellison*. Available online.

Karp P and Taylor J (2019) Police made illegal metadata searches and obtained invalid warrants targeting journalists. *The Guardian*. Available online.

Keane B (2015) Your guide to the metadata retention debate what it is and why. *Crikey*. Available online.

Kirby M (2021) The changing legal framework of the Australian Intelligence Community: From Hope to Richardson. *Alternative Law Journal, 95*, 1–14.

Knaus C (2021) Friendlyjordies arrest by NSW police fixated persons unit questioned by former top prosecutor. *The Guardian*. Available online.

Knowles L, Worthington E, and Blumer C (2019) ABC raid: AFP leave Ultimo building with files after hours-long raid over Afghan Files stories. *ABC News*. Available online.

Lashmar P (2017) No More Sources? *Journalism Practice* 11(6): 665–688

Lee M and Heinrichs R (2019) How to protect the truth? Challenges of cybersecurity, investigative journalism and whistleblowing in times of surveillance capitalism. An interview with Micah Lee. *Ephemera: Theory & Politics in Organization* 19(4): 807–824

Lindberg KS (2021) Nearly Half of Hong Kong's Reporters Mulling Exit Survey Finds. *Bloomberg*. Available online.

Loomes P (2021) Infamous far-right YouTube personality Avi Yemini rants from police van after being detained on Australia Day. *News.Com.Au*. Available online.

Lyons J (2019) AFP raid on ABC reveals investigative journalism being put in same category as criminality. *ABC News*. Available online.

Mann M & Murray A (2021) Striking a balance: Legislative expansions for electronic communications surveillance in Australia. *Precedent, 166*, 44–51

Mann M & Daly A (2019). (Big) data and the north-in-south: Informational imperialism and digital colonialism in Australia. *Television and New Media, 20*(4), 379–395.

MEAA (2015) Submission to the Senate Legal and Constitutional Affairs References Committee into the Comprehensive revision of the Telecommunications (Interception and Access) Act 1979. Available online.

MEAA (2021) *MEAA Journalist Code of Ethics*. Available online.

Murray A and Mann M (2020) *Submission to PJCIS regarding Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*. Australian Privacy Foundation. Available online.

Murray R, Ananian-Welsh R, & Greste P (2021) Journalism on Ice - National Security Laws and The Chilling Effect in Australian Journalism. In T. Workneh & P. Haridakis (Eds.), Counter-Terrorism Laws and Freedom of Expression: Global Perspectives (pp. 295–317). Lexington Books.

Parliamentary Joint Committee on Intelligence and Security (2020a) *Review of the mandatory data retention regime*. Available online.

Parliamentary Joint Committee on Intelligence and Security (2020b). *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*. Available online.

Paynter J (2021) Herald Sun journalist, photographer arrested at Melbourne anti-vax protests. *The Australian*. Available online.

Ping L (2019) Surveillance, Harassment 'The New Normal' For Foreign News Organizations in China. *Radio Free Asia*. Available online.

Posetti J (2017) Protecting journalism sources in the digital age: UNESCO Publishing.

Posetti J (2018) The Future of Investigative Journalism in an Era of Surveillance and Digital Privacy Erosion. In (pp. 249–261): Springer International Publishing.

Posetti J, Dreyfus S, and Colvin N (2019) *The Perugia Principles for Journalists Working with Whistleblowers in the Digital Age*. Blueprint for Free Speech. Available online.

Rebel News (2021) Avi Yemini OWNS police who tried to ARREST him today at lockdown protest. *Youtube: Rebel News*. Available online.

Remeikis A (2018) Australian bill to create back door into encrypted apps in 'advanced stages'. *The Guardian*. Available online.

Roach K (2011) *The 9/11 Effect: Comparative Counter-Terrorism*. UK: Cambridge University Press.

RSF – Reporters without Borders (2021) *European Court of Human Rights admits RSF complaint against the BND's mass surveillance.* Available online.

SecureDrop (2021) About SecureDrop: Frequently asked questions about SecureDrop and its security. Available online.

Sky News (2019) Fordham may face AFP raid. *Sky news*. Available online.

Staub Z (n.d.) Five reasons why Australia should adopt a statutory national Bill of Rights. *Australian Human Rights Institute*. UNSW. Available online.

Stilgherrian (2021) The Encryption Debate in Australia: 2021 Update. *Carnegie Endowment for International Peace*. Available online.

Stuart T (2021) 'Bitter,' 'Angry,' 'Enraged': Reality Winner Blasts the Intercept After 4 Years in Jail. *Rolling Stone*. Available online.

Suzor N, Pappalardo K, and McIntosh N (2017) The passage of Australia's data retention regime: national security, human rights, and media scrutiny. *Internet Policy Review: Journal on Internet Regulation* 6(1)

Taylor J (2019) Australian federal police accessed journalists' metadata 58 times in a year. *The Guardian*. Available online.

Taylor J (2020a) Web browsing histories are being given to Australian police under data retention powers. *The Guardian*. Available online.

Taylor J (2020b) Australian government officials accused of 'cavalier disregard' for unauthorised metadata access. *The Guardian*. Available online.

The Parliament of The Commonwealth of Australia (2020). Addendum to the Explanatory Memorandum of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (Cth). Available online.

Tsui L (2019) The importance of digital security to securing press freedom. *Journalism* 20(1): 80–82.

Tsui L and Lee F (2021) How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom. *Journalism* 22(6): 1317–1339

Wilson C (2021) Australia's anti-encryption law costs billions and hurts our reputation — just as the industry warned. *Crikey*. Available online.

Woodman S (2018) Five digital security tools to protect your work and sources. *International Consortium of Investigative Journalists*. Available online.

Wroe D (2017) How the Turnbull government plans to access encrypted messages. *The Sydney Morning Herald*. Available online.

Legislation Cited

Telecommunications (Interception and Access) Act 1979 (Cth)

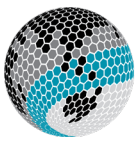
Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth)

International Information Sharing (Telecommunications Legislation Amendment (International Production Orders) Act 2021 (Cth)

Securing Australian Journalism from Surveillance



ADI
ALFRED DEAKIN INSTITUTE FOR
CITIZENSHIP AND GLOBALISATION