Submission to Joint Parliamentary Committee on Law Enforcement

Inquiry into new Information Communication Technologies (ICTs) and the challenges facing law enforcement agencies.

Joint submission by Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly

on behalf of the Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia, and Future Wise.

Australian Privacy Foundation

Digital Rights Watch

1. Executive summary

After summarising our expertise in new Information Communication Technologies (ICTs) and law enforcement, this submission provides:

- An overview of the context which underscores the need to consider the relationship between Australian law enforcement and new ICTs;
- Examination of the key issues relating to this relationship in the following areas, as aligned with our expertise:
    - 3D printing technologies with specific reference to firearms;
    - Transnational policing with reference to issues of jurisdiction and extraterritoriality and policing of cryptomarkets in the dark web;
- Key issues in developments in ICTs and Australian law enforcement, including:
    - Mandatory data retention;
    - Suggestions to weaken encrypted communications;
    - Big data and algorithmic policing;
    - Biometrics, specifically facial recognition;

We conclude with a summary of key issues and a list of recommendations for consideration by the Joint Parliamentary Committee on Law Enforcement. At the end of this submission we present a list of key publications of the four contributors that elaborates on each of the issues presented.

Recommendations

Our main recommendations as regards to new ICTs and the challenges facing law enforcement are:

1. Follow international precedent in surveillance programs and practices and with regard to, and respect of, international human rights standards;
2. Suspend the current program of mandatory data retention and require a judicial warrant to access telecommunications information;
3. Do not implement law or practices that involve undermining or weakening encrypted forms of communication and make use of existing targeted powers for accessing telecommunications information (via a judicial warrant as per the recommendation immediately above);
4. In the case of investigations with an extraterritorial element, Australian police procedures comply with established MLAT procedures;
5. Implement standards and procedures to ensure both the admissibility of evidence and the integrity of transnational investigations;
6. Implement appropriate oversight structures for police use of new ICTs;
7. Gather robust independent evidence on which reforms to law and policing on the basis of new technologies are guided and based, and;
8. Increased government funding for independent research should be made available on a competitive basis.

2. Background and expertise

This is a joint submission by Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly. We are the leading Australian experts working on the intersections of technology, regulation, law, crime and policing. Both individually, and collectively as a research team, we have published widely across the issues of surveillance, intelligence, biometrics, new investigative techniques for online policing, transnational online policing, the dark web and cryptomarkets (drugs and child exploitation material), 3D printing technology including firearms, commercial and government use of spyware, telecommunications and cyber security policy, and the associated legal and human rights implications of new and emerging technologies and their applications in contemporary law enforcement.[1] Moreover, we represent and maintain leadership positions in the main privacy and digital rights civil society organisations in Australia including the Boards of the Australian Privacy Foundation and Digital Rights Watch Australia.

We appreciate being invited to provide this submission to the Joint Parliamentary Committee on Law Enforcement Inquiry into new ICTs and the challenges facing law enforcement under the inquiry's terms of reference:

a. challenges facing Australian law enforcement agencies arising from new and emerging ICT;
b. the ICT capabilities of Australian law enforcement agencies;
c. engagement by Australian law enforcement agencies in our region;
d. the role and use of the dark web;
e. the role and use of encryption, encryption services and encrypted devices; and
f. other relevant matters.

In this submission we first describe the context in which current developments are situated. We then examine both the impact of new ICTs on crime and law enforcement use of new ICTs. Finally, we outline the main issues and concerns and present our recommendations.

3. Context and arguments

There have been attempts by governments around the world, including the Commonwealth Government, to harness data and new ICTs for more efficient delivery of systems and services but there have been a number of examples where this has gone awry (RoboDebt,[2] 2016 Census,[3] or the release of readily re-identifiable data[4]).

[1]Refer to the bibliography of author works presented at the conclusion of this document. We will provide full copies upon request from the Committee Secretary.
[2] Community Affairs References Committee (2017). Senate inquiry into the design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative. Canberra: Commonwealth of Australia.
[3] Mann, M. and Rimmer, M. (2016). Submission to the Senate Economics References Committee on the 2016 Census. Retrieved from: https://eprints.qut.edu.au/99687/
[4] Teague, V., Culnane, C., and Rubinstein, B. (2017). The simple process of re-identifying patients in public health records. University of Melbourne. Retreived from: https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records

Moves towards increasing digitisation of public service is especially apparent in law enforcement and policing contexts. The National Commission of Audit[5] recommended the merger of the Australian Crime Commission (ACC) with the CrimTrac Agency forming the Australian Criminal Intelligence Commission (ACIC). This clearly demonstrates the increasing importance and emphasis that is being placed on data-led policing in Australia, at a time where there are pressures on resource allocation and productivity. More data is viewed as a way of increasing police efficiency, productivity and effectiveness.[6]

There is little empirical evidence supporting these 'common-sense' assertions; a reoccuring theme when it comes to the impact of technology on both crime and policing, and the efficacy of the uses of technology in police work. This is compounded by a tendency to 'balance' individual rights against claims of increased effectiveness in protecting national security. This is a false trade-off, particularly where many uses of new technologies are unregulated or untested.[7]

Technology is not a panacea for policing new and emerging forms of crime facilitated by technology. Rather, a number of additional issues and concerns are introduced, particularly that of ensuring individual rights (whether they be human rights such as privacy) or due process rights (such as presumption of innocence, and reasonable suspicion) are protected.

We recognise that with new technology comes new opportunities to commit crime (and new categories of crime) and also new challenges for policing. However, these challenges need to be met in a way that is consistent with the rule of law and international human rights standards. We argue that law enforcement use of ICTs needs to be met with appropriate safeguards and robust oversight structures and that they need to be implemented before widespread adoption of new technologies in policing. Where relevant we detail specific practical reforms to address this imbalance.

4. Impact of new and emerging ICT on crime and policing

New and emerging decentralised ICTs create new challenges for law enforcement including complex cross-jurisdictional criminal offending and the use of widely available tools for anonymisation. In this section we examine the main disruptive ICTs for crime and policing, aligned with our fields of expertise.

[5] National Commission of Audit. (2014). *The report of the National Commission of Audit.* Retrieved from National Commission of Audit website: http://www.ncoa.gov.au/report/index.html

[6] Mann, M. (2016). New public management and the 'business' of policing organised crime in Australia. *Criminology and Criminal Justice, 17*(4), 382-400. doi: 10.1177/1748895816671384

[7] Mann, M., Daly, A., Wilson, M. and Suzor, N. (in press, 2018). The limits of (digital) constitutionalism? Exploring the privacy-security (im)balance in Australia. *International Communication Gazette,* Retrieved from https://ssrn.com/abstract=3021580; Palmer, D., Warren, I. and Miller, P. (2013). ID-scanners in the night-time economy: Social sorting or social order? *Trends and Issues in Crime and Criminal Justice no. 466*. Retrieved from the Australian Institute of Criminology: http://www.aic.gov.au/publications/current%20series/tandi/461-480/tandi466.html

3D printing technology, especially firearms

A clear example how new ICTs present disruptions to criminal law and policing can be found in relation to 3D printed firearms. 3D printing and the Internet, as decentralised technologies, present challenges to the design of various areas of law and their effective enforcement, including criminal laws.[8] With the development and distribution of design files for a functioning gun that can be printed on a cheap 3D printer now accessible on the dark net and other file sharing sites, the possibility of manufacturing illegal weapons has been realized for anyone with an Internet connection and a 3D printer.

However, there is limited robust evidence about the extent to which such 3D printed firearms are being made and used in practice (Daly and Mann are currently conducting the first global empirical study of 3DP technology and policing in collaboration with the Global Complex for Innovation at Interpol, IGCI). There have been a few reports of 3D printed guns, suspected gun parts and other 3D printed items being detected in Australia and other countries internationally. There has been interest in the capabilities of 3D printers from police forces, notably the NSW police which purchased a printer to create their own 3D printed firearm, which they viewed to be as dangerous to the person holding the gun as the person to whom the gun may be directed, due to the low quality of the printed object.

NSW is also the leading jurisdiction internationally which has introduced new offences relating to 3D printed firearms and design files. Many jurisdictions' laws and offences regarding the unlicensed manufacture, creation and possession of firearms will cover 3D printed firearms, although not necessarily the possession or distribution of design files. The extent to which a new offence is necessary is not yet proven, especially in the current scenario where few instances of illicit 3D printed firearms are being detected by police.

At the moment, there is very little robust evidence about the extent to which 3D printers are currently being used to manufacture illicit firearms, both in Australia and internationally. Research should determine the shape and size of the potential threat, and what possible legal and policing responses should be. Presently, it appears that 3D printers are being used to create many more socially-beneficial items than dangerous ones, and so legal and policing responses which may restrict these socially-beneficial uses should not be implemented until they are informed by better evidence. The extent to which the NSW offences related to 3D printed firearms are necessary should be monitored before other measures are introduced elsewhere.

Transnational policing: Jurisdiction and extraterritoriality

New ICTs present several challenges for the collection of digital evidence that may be stored extraterritorially in cloud computing services or on commercial servers located in other jurisdictions. The common concern is the transnational nature of the internet and electronic data flows now render national geographic borders irrelevant.[9] This creates problems for digital service providers (that operate globally) in complying with different national laws and

[8] Daly, A. (2016). *Socio-Legal Aspects of the 3D Printing Revolution*. UK: Palgrave Macmillan.
[9] Daskal, J. (2015). The un-territoriality of data. *The Yale Law Journal 125*(2), 328-398. Retrieved from https://www.yalelawjournal.org/article/the-un-territoriality-of-data

frameworks that govern criminal investigations.[10] However, it also has important implications for contemporary policing, given the jurisdictional authority for law enforcement activity is traditionally determined by physical geography or territory.

The policing of transnational online activity associated with online child exploitation, drug trafficking, people smuggling and other real-world activities is undertaken primarily at a domestic level, or via international cooperative methods that are enacted through domestic laws, procedures and guidelines. It is incorrect to assume that the Internet renders national borders irrelevant, as the laws associated with transnational evidence exchange conform to established international and domestic law requirements governing the legitimate scope of law enforcement jurisdiction. The perception that the cyber-domain is largely ungoverned or ungovernable is because of the complexity of online investigations and existing transnational methods of police cooperation. In fact, this perception fuels highly questionable policing, surveillance and information exchange processes that are subject to minimal external scrutiny or independent review.[11] The main areas where jurisdiction impacts criminal investigations and that will be considered in this section are:

- access and seizure of evidence located in offshore servers, or conveyed through multiple geographic points by multiple internet service providers (ISPs), many of which will not be affiliated with domestic service providers in Australia;
- the admissibility of such evidence in criminal trials;
- seizure and/or operation of dummy websites (or 'watering holes') to apprehend online offenders if the original site is located offshore or is operated through the Dark Web, and;
- the role of Mutual Legal Assistance Treaties (MLATs) in these processes.

MLATs create a formally recognised structure for the exchange of physical and digital evidence between jurisdictions, but do not generally cover the legalities or ethics of the extraterritorial seizure and operation of websites. It is widely recognised that MLATs are cumbersome, time consuming and inefficient, with potential to delay, limit and compromise the collection of digital evidence in cases involving serious forms of transnational criminal offending.[12] However, domestic law enforcement agencies must follow established MLAT processes in order to protect individual and due process rights, and to ensure evidence is admissible in domestic criminal trials.

MLATs operate in a similar way to the transfer of people under the processes of extradition, where:

- the state seeking the information (the requesting state) makes a formal request to authorities in the jurisdiction where the evidence is physically located (the requested state);
- officials in the requested state assess the merits of the request, and, if satisfied the request complies with local due process requirements, will issue a warrant to conduct a search and to seize relevant evidence;

[10] Svantesson, D. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford: OUP.
[11] Bowling, B. and Sheptycki, J. (2015). Global policing and transnational rule with law. *Transnational Legal Theory 6*(1), 141-173. doi: 10.1080/20414005.2015.1042235
[12] Ibid.

- once seized under the authority of the local warrant, the evidence is transferred to the requesting state for use in its domestic procedures.

MLAT requirements directly incorporate provisions for conducting searches and seizures, which are often unquestioned in domestic police and criminal procedures. The limits associated with a warrant requirement, including the need for *prima facie* evidence to be scrutinised by a judge or magistrate, are frequently sidestepped in transnational contexts, because these procedures are new or poorly tested in the courts.[13] However, they are also of central international importance, as the unilateral collection of evidence by one nation can have significant political and diplomatic ramifications if it is believed that the sovereignty of another nation is negatively affected.

Laws governing police procedure with transnational digital evidence must reconcile two tensions that are currently incorporated into the MLAT process:

> i. the need avoid the prospect of unilateral action by the requesting state and thus preserve, as far as possible, the jurisdictional integrity of the requested state; and
>
> ii. the need to ensure t clear limits on law enforcement surveillance activity to protect the rights of crime suspects, regardless of their geographic location during the course of the investigation.

The laws governing the search of premises or property and the seizure of evidence that customarily apply in domestic criminal prosecutions require greater clarity in a transnational context. This is particularly so given the perceived urgency of many criminal investigations involving clandestine online activity, including those involving child exploitation.[14]

These issues have been of particular concern in the United States of America (USA), where there are growing demands for extraterritorial policing operations in cases involving a connection with domestic corporation or crime control issues. Most leading global internet and cloud computing services are developed and administered by US corporations.[15] There is an ongoing and unresolved legal issue regarding the permissible scope of law enforcement access to digital evidence that is located extraterritorially and that remains under the control of US corporations.[16]

The Microsoft Warrant case is scheduled for hearing in the in the US Supreme Court in June 2018[17] and will determine whether US federal authorities can lawfully access data stored by

[13] Bowling, B. and Sheptycki, J. (2015). Global policing and transnational rule with law. *Transnational Legal Theory 6*(1), 141-173. doi: 10.1080/20414005.2015.1042235
[14] Ghappour, A. (2017). Searching places unknown: Law enforcement jurisdiction on the dark web. *Stanford Law Review 69*(4), 1075-1136. doi: 10.2139/ssrn.2742706
[15] Mann, M. and Warren, I. (2018). The digital and legal divide: *Silk Road*, transnational online policing and Southern criminology. In K. Carrington, R. Hogg, J. Scott and M. Sozzo (Eds.) *The Palgrave Handbook of Criminology and the Global South* (pp. 245-260). Springer: Cham, Switzerland.
[16] Warren, I. (2015). Surveillance, criminal law and sovereignty. *Surveillance and Society 13*(2), 300-305. Retrieved from https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/law_sovereign/law_sov.
[17] The Australian Privacy Foundation, with Privacy International and other international human and digital rights watch organisations, has submitted an Amicus Brief to the US Supreme Court in support of Microsoft. This can be retrieved from the US Supreme Court Docket:

Microsoft in a server located in Ireland to assist in a domestic criminal investigation, independently of the MLAT requirements. However, commentary surrounding this case fails to acknowledge the suspect involved is an *Irish national* located in *Ireland* at the time of the allegedly unlawful act, who has been subject to protracted appeals governing extradition that depend on the US Supreme Court's ruling.[18] To date, federal appeal courts have determined data access independently of the MLAT between the US and Ireland depends on the level of control the private internet service provider has over the information. Prior federal appeal courts have held that Microsoft is obliged to hand over the information regardless of where it is stored, because, as a US corporation, it controls that information. A contrary interpretation of this issue suggests that a MLAT is required because the server on which the data is stored is located in another jurisdiction, and involves a suspect who is also located outside of the US.

These legal grey areas ultimately compromise police investigations into complex transnational crimes. However, they are not unique to the US or to the online environment. For example, there are numerous historical cases involving questionable police tactics in installing surveillance devices without a warrant to assist foreign law enforcement agencies in tracking vessels suspected of involvement in transnational drug trafficking activity.[19] More recently, the high profile New Zealand (NZ) case concerning Kim Dotcom highlights the complexities of the MLAT procedure on enforcement agencies seeking to cooperate with international partners.[20] Specifically, a series of procedural anomalies associated with how the US MLAT request was operationalised by NZ Police have called into question the legality of the methods used to seize the data, even if that data is likely to be declared admissible in a US court.[21] These issues have consumed the NZ courts for five years, and many remain unresolved, although several rulings have favoured Kim Dotcom's arguments that he was subject to unlawful surveillance activity that has compromised the integrity and legality of the entire investigation. This resource drain results from a failure of NZ Police to fully comply with relevant domestic policing standards, which ultimately complicates the integrity of the bilateral cooperative procedures under the MLAT.

A final issue of concern involves determining the appropriate scope for transnational police cooperation. Although there are few examples to draw on, recent experience in the European union highlights the collapsing of national jurisdictional borders has significant implications on the due process rights of European citizens and residents. This is particularly evident in the enforcement of the European Arrest Warrant and the European Evidence Warrant. These methods of streamlining enforcement cooperation are also backed by a process of judicial review and a sophisticated human rights framework under the European Convention of

---

https://www.supremecourt.gov/DocketPDF/17/17-2/28354/20180118170547648_17-2%20USA%20v%20Microsoft%20Brief%20of%20Privacy%20International%20Human%20and%20Digital%20Rights%20Organizations%20and%20International%20Legal%20Scholars%20as%20Amici%20Curiae%20in%20Support%20of%20Respondent.pdf

[18] Mann, M., Warren, I. and Kennedy, S. (forthcoming). The legal geographies of transnational cyber-prosecutions: Extradition, human rights and forum shifting. *Global Crime* (accepted for publication, November 2017); Mann and Warren (2018).

[19] Warren, I. and Palmer D. (2015). *Global Criminology*. Pyrmont NSW: Thomson Reuters/Law Book Company.

[20] Palmer, D. and Warren, I. (2013). Global Policing and the Case of Kim Dotcom. *International Journal For Crime, Justice And Social Democracy, 2*(3), 105-119. doi: 10.5204/ijcjsd.v2i3.105

[21] Warren, I. and Palmer D. (2015). *Global Criminology*. Pyrmont NSW: Thomson Reuters/Law Book Company, 73-80.

Human Rights and European Court of Human Rights. However, these measures are also criticised for removing consideration of the defendant's due process and privacy rights.[22]

Similarly, recent literature points to the need to consider the 'effect' of the allegedly unlawful conduct in determining the appropriate jurisdiction for accessing evidence and commencing a prosecution.[23] The difficulty with this proposition is it does little to regulate police standards, or recognise that territorial controls on police conduct are important in protecting suspects from unbridled transnational surveillance. As our recommendations demonstrate, debates about transnational surveillance for law enforcement purposes require clear rules to set standards for the conduct of the investigation and admissibility of evidence, with the 'effects test' often leading to a 'first-come-first-served' scenario that is not always amenable to protecting the rights of crime suspects.[24]

Cryptomarkets and policing the 'dark-web'

Increasingly, investigations involve extraterritorial police activity through a Computer Network Operation (CNO) or Network Investigation Technique (NIT). Law enforcement are collecting information from all over the world by taking over illegal marketplaces that traffic in child exploitation material (such as *Playpen*) or drugs (such as the *Silk Road*). Without proper checks, police could have significantly expanded scope to search computers and this is creating troubling new standards in transnational policing. New rules for digital evidence collection and exchange must be developed to assist prosecutions while preserving due process and human rights.

These types of operations on the dark web involve:

- seizure of the offending website;
- a 'honeypot' or 'watering hole' operation that involves keeping the site in operation, but filtering all activity through a law enforcement server (located in *any* domestic jurisdiction);
- automatically sending malware (the CNO or NIT) to any person logging into the site that provides law enforcement agents with:

    - the IP address of any computer that logs in, and the date and time it was used to enter the site;
    - a unique identifier to distinguish a target computer from other computers using or linked to the dummy site;
    - the target computer's operating system and active operating system username;
    - the computer's host name; and
    - the computer's media access control address.

[22] Gless, S. (2015). Bird's-eye view and worm's eye view: Towards a defendant-based approach in transnational criminal law. *Transnational Legal Theory* 6(1): 117-140. Retrieved from https://ssrn.com/abstract=2724571
[23] Svantesson, D. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford: OUP.
[24] Parrish, A. (2008). The effects test: Extraterritoriality's fifth business. *Vanderbilt Law Review 61*(5), 1455-1505. Retrieved from https://ssrn.com/abstract=1099485

While the legality of these processes is unclear and subject to ongoing litigation in the US surrounding the detection and clandestine operation of the Playpen website, Australian law enforcement agencies have been involved in similar investigations.[25]

At present, there is limited regulatory guidance for the use of CNO/NIT procedures in any jurisdiction, including Australia. Some commentators (including ourselves) are highly critical of the government sponsored use of malware, particularly due to its extraterritorial effects, which are in turn complicated by the cumbersome and inconsistently applied procedures for evidence exchange under MLATs.[26] Others disagree, indicating that states involved in justifiable law enforcement investigations are unlikely to meet with international resistance given the shared concern for Dark Web criminal activity, and specifically child exploitation material. Similarly, decisions to deploy a CNO/NIT are frequently reviewed through administrative processes within law enforcement agencies and have become common practice in complex police operations within the Dark Web.[27] However, such decisions are seldom open to judicial oversight, or independent review until after a prosecution has commenced.

At a minimum, the power to seize and operate a website located offshore should involve:

- consent from law enforcement agencies and relevant government authorities where the site / server hosting the site is located;
- appropriate time limits for the collection of information through a CNO/NIT;
- appropriate requests via locally operated ISPs, or, where suspects are located offshore, a documented evidence exchange procedure with authorities where the suspect computer is located; and
- clear standards for the admissibility of exchanged evidence based on these documentary records.

This will help to avoid the prospect CNO/NIT investigations becoming unilateral enforcement decisions without independent judicial oversight in either the requested or requesting jurisdictions.

5. Law enforcement use of new and emerging ICTs

New and emerging ICTs create new opportunities, but also new risks, for use in law enforcement and intelligence contexts. Law enforcement use of new ICTs should be supported with evidence, consistent with international human rights standards, subject to robust oversight and proper checks and balances and uphold the rule of law. In Australia, however, this is frequently not the case. In this section, as aligned with our expertise, we examine problematic law enforcement use of new and emerging ICTs.

[25] Warren, I., Molnar, A. and Mann, M. (2017, September 7). Poisoned water holes: The legal dangers of dark web policing. *The Conversation.* Retreived from https://theconversation.com/poisoned-water-holes-the-legal-dangers-of-dark-web-policing-82833

[26] Ghappour, A. (2017). Searching places unknown: Law enforcement jurisdiction on the dark web. *Stanford Law Review 69*(4), 1075-1136. doi: 10.2139/ssrn.2742706

[27] Kerr, O.S. and Murphy, S.D. (2017). Government hacking to light the dark web: What risks to international relations and international law? *Stanford Law Review 70*(1), 58-63. Retrieved from https://www.stanfordlawreview.org/online/government-hacking-to-light-the-dark-web/

Mandatory data retention

The continued program of mandatory data retention is at odds with international precedent that has ruled these powers are a disproportionate interference with individual rights. These laws allow authorised law enforcement agencies warrantless access to all citizens' digital information. The civil society organisations that we represent have made numerous submissions to public inquiries into these laws and we will not repeat or rehash these arguments again here.[28] However, we take this opportunity to note that ongoing developments particularly in the European Union and domestically in the United Kingdom have shown that mandatory data retention schemes which permit warrantless access are not compliant with procedural justice and human rights norms. The emerging international human rights view is that such schemes are not compatible with the rights to privacy and free expression recognised in treaties such as the International Covenant for the Protection of Civil and Political Rights (ICCPR) which Australia has signed and ratified.

The fact that even the journalists' warrant process in the Australian scheme has not been followed by the Australian Federal Police (AFP), by their own admission, is highly concerning from a due process and rule of law perspective. Given these deficiencies, Australia's mandatory data retention scheme should be discontinued immediately, and warrants must be sought and obtained from independent judicial authorities before law enforcement agencies can accessed individuals' digital information.

Encryption and 'lawful access'

Governments have made frequent public statements regarding law enforcement and intelligence agencies' collection capabilities 'going dark' as a consequence of the use of encrypted messaging applications and other forms of encrypted electronic communication. The rationale behind this argument is that encrypted messaging apps are having detrimental impacts on their ability to prevent, detect and investigate serious crimes such as terrorism and the distribution of child exploitation material.[29] Accordingly, these agencies insist that further powers are needed to enable access to encrypted communications.

Similar concerns have also been raised by the Australian government, with Prime Minister Turnbull stating that "the laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia ... I am not a cryptographer...but what we are seeking to do is secure their assistance."[30] This remark gestures at an impending legislative proposal in Australia that would introduce provisions to potentially weaken or undermine end-to-end

[28] Lindsay, D.F., Greenleaf, G., Daly, A., Waters, N., Molnar, A. and Vaile, D. (2015). Australian Privacy Foundation Submission on the Data Retention Bill 2014. doi: 10.2139/ssrn.2553652

[29] Comey, J.B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*. Federal Bureau of Investigation Speeches. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course; see also
Comey, J.B. (2016). *Encryption Tightrope: Balancing Americans' Security and Privacy*. Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy

[30] Roberts, R. (2017, July 15). Prime Minister claims laws of mathematics 'do not apply' in Australia. *The Independent*. Retrieved from https://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-of-mathematics-do-not-apply-australia-encryption-l-a7842946.html.

encryption tools.[31] At present, it is unclear if Australia's laws will require so-called 'backdoor' vulnerabilities to be built into messaging applications like Facebook Messenger and WhatsApp, or Apple products, and whether this step would require these companies to modify their products and services in Australia or consider removing them from the domestic market altogether. This is a policy problem that requires careful and informed deliberation.

In spite of any claims that end-to-end encryption tools introduce insurmountable obstacles for intelligence gathering and criminal investigation, we insist that our present digital age offers an unparalleled opportunity for intelligence gathering and criminal investigation compared with any previous point in history.[32] Australian authorities already have extensive technical and legal capabilities at their disposal to gather, store, and analyse social and geolocational data to facilitate operations. This includes surveillance authorised via the *Telecommunications (Interception and Access) Act 1979* (Cth), the *Surveillance Devices Act 2004* (Cth) the mandatory metadata retention regime as described immediately above, and also Computer Network Operations authorised by Section 25(a) of the *Australian Security Intelligence Organisation Act 1979* (Cth). This is not to mention the extensive and shadowy surveillance practices of the Five Eyes alliance (of which Australia is a partner) as exposed by Edward Snowden's revelations.

In spite of this 'golden age' for intelligence and criminal investigation capabilities, a number of proposals have been advanced as a way to undermine the use of, and weaken, encryption tools. They span a range of activities such as the censorship or banning of end-to-end encrypted messaging tools (in countries such as Iran, Turkey, and potentially Australia[33]), export controls[34], or criminalisation of the research and development of encryption tools.[35] We have serious misgivings about these approaches and note that they carry a net effect of weakening the security of digital communications generally, criminalising activities that are important for maintaining public safety, cyber security and digital innovation, and carry significant negative impacts on the human rights of individuals (especially privacy, freedom of expression), the private sector, and government.[36]

---

[31] Prime Minister of Australia. (2017, July 14). Press Conference with the Attorney-General, Senator the Hon. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr Michael Phelan APM [press release]. Retrieved from http://www.pm.gov.au/media/2017-07-14/press-conference-attorney-general-senator-hon-george-brandis-qc-and-acting

[32] Swire, P. and Ahmad, K. (2011, November 8). 'Going Dark' Versus a 'Golden age for Surveillance'. *Center for Democracy and Technology*. Retrieved from https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/

[33] Brandom, R. (2018, January 2). Iran blocks encrypted messaging apps amid nationwide protests. *The Verge.* Retrieved from https://www.theverge.com/2018/1/2/16841292/iran-telegram-block-encryption-protest-google-signal; Uras, U. (2015, September 2). Vice News fixer 'charged over encryption software'. *Aljazeera.* Retrieved from http://www.aljazeera.com/news/2015/09/vice-news-fixer-arrested-encryption-software-150901200622345.html

[34] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996) Wassenaar Arrangement Secretariat, Vienna, Austria. Retrieved from http://www.wassenaar.org/

[35] Vagle, J. 2015. Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance. *Indiana Law Journal*. Retrieved from http://ilj.law.indiana.edu/articles/11-Vagle.pdf

[36] Kaye, D. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN Doc A/HRC/29/32). Retrieved from United Nations Human Rights Council website http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

There are also a number of activities that are geared towards gaining access to the plaintext of encrypted data that weaken and undermine encryption at a network level. These include:

- regulations to weaken encryption standards (algorithmic protocols) that are relied upon by end-users such as individuals, the private sector, and government in ways that continue to ensure access is facilitated by law enforcement and security intelligence agencies.[37]
- regulations to establish a 'key escrow' system where the decryption key is held by government, third-party entity, or combination therein, which is used under 'exceptional' circumstances to recover the plain text[38]
- mandatory decryption obligations for telecommunications service providers
- mandating the deliberate introduction of vulnerabilities in the design of digital communications products and services[39]

Again, we have serious misgivings about these proposals. While it might be the case that such proposals may facilitate law enforcement access to communications at a network-level scale, they will similarly do so for criminal hackers, organised criminals, or foreign state actors who acquire access. Computer scientists have noted that any introduction of a 'backdoor' vulnerability for law enforcement and security intelligence will similarly do so for malicious actors.[40] Resorting to any of these policy proposals that attempt to weaken or undermine the design, standards, or protocols of encryption at a network level would introduce serious risks for a range of individuals (journalists, human rights advocates, ordinary consumers), the private sector (finance, commerce), and government.

As noted in Access Now's submission to this inquiry,[41] we would like to echo the significant public value that encryption holds for social, economic, and public safety uses. Further, there are many legitimate and socially desirable uses of encryption which are likely to be adversely affected by weakening encryption.[42] Encryption has been used to protect fundamental rights such as privacy and free expression and there have been calls for strong encryption to be recognised as a human right in and of itself.[43]

The ACIC estimates that identity crime is "more common than robbery, motor vehicle theft, household break in, or assault," impacting approximately 5% of Australia's population (970,000 people), with an estimated cost to victims, business, and government agencies of at

[37] Kaye, D. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN Doc A/HRC/29/32). Retrieved from United Nations Human Rights Council website http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx

[38] Abelson H. et. al. (1997). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. *World Wide Web Journal, 2*(3): 241-257. Retrieved from https://www.schneier.com/academic/paperfiles/paper-key-escrow.pdf

[39] Abelson H. et. al. (2015). Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. *Journal of Cybersecurity, 1*(1), 69-79. doi: 10.1093/cybsec/tyv009.

[40] Schneier, B. (2016, January 25). Business Report How an Overreaction to Terrorism Can Hurt Cybersecurity. *MIT Technology Review.* Retrieved from https://www.technologyreview.com/s/545716/how-an-overreaction-to-terrorism-can-hurt-cybersecurity/

[41] Access Now submission to PJC Inquiry into new ICTs and the challenges facing law enforcement agencies. Retrieved from: https://www.aph.gov.au/DocumentStore.ashx?id=285d117c-9bc1-41c9-b941-600c7cea35cb&subId=562322

[42] Abelson H. et. al. (2015). Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. *Journal of Cybersecurity, 1*(1), 69-79. doi: 10.1093/cybsec/tyv009.

[43] Schulz, W., & van Hoboken, J. (2016). *Human Rights and Encryption.* UNESCO Series on Internet Freedom. Paris, France: UNESCO. Retrieved from http://unesdoc.unesco.org/images/0024/002465/246527E.pdf

least $2.2b per year.[44] There is every reason to believe that the aforementioned policy proposals will have a damaging influence on the prevention of identity theft in Australia.

Given the risks posed by these proposals, it is also essential to recognise that end-to-end encryption tools do not pose a fatal hurdle for security intelligence and criminal investigation. Australian officials already have at their disposal a range of technical and legal powers to address the issue of 'going dark.' Importantly, these powers are more selective and targeted, and are considered to be less prone to disproportionate trade-offs in network-level security. They include:

Existing powers for lawful authorities to compel passwords

- Amendments to the *Cybercrime Act 2001* (Cth) introduced a new section 3LA under the *Crimes Act 1914* (Cth) to provide law enforcement officers power to issue an 'assistance order' that would compel an individual to reveal private passwords for the purposes of investigating and prosecuting an offence. Failure to comply with this request is punishable by up to six-month's imprisonment. While we note problems with this approach when it comes to procedural justice (ie., the violation of an individual's right against self-incrimination)[45] compared with other jurisdictions that have a constitutional rights framework, this statute can be used to broker access to compel private decryption of information on contained lawfully seized devices. If this approach is to be relied upon, we insist that these powers are necessarily justified, carefully targeted, and when other less intrusive means of investigation are not available.

Existing powers to facilitate targeted hacking of end-point devices

- Australian security intelligence and law enforcement authorities already have extensive existing legal and technical powers to selectively target and hack end-point devices as a way to access plain-text communications. [46] These laws include powers to use CNOs under judicial authorisation, such as a phishing attack to acquire access to encrypted messages.
- While we recognise that the current Australian legislative powers to hack end-point devices occurs under existing legal frameworks are at present incompatible with rule of law, due process, and constitutional human rights frameworks[47], some jurisdictions, such as Germany, are opting to develop legal frameworks to facilitate targeted end-point hacking rather than adopting policies that would weaken or undermine encryption at a network-level in ways that would be exponentially more harmful to the security and safety of individuals, the private sector, and the government.[48]

---

[44]Attorney-General's Department Australian Government. (2016). *Identity crime and misuse in Australia 2016*. Retrieved from Attorney-General's Department website https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-crime-and-misuse-in-Australia-2016.pdf

[45] 5th amendment, right to not self-incriminate

[46] Part 2.2 and 2.5 Warrants under the Telecommunications Interception and Access Act 1979; Surveillance Devices Act (2004); ASIO Act 1979, s.25a, see 'computer access warrants'

[47] For more info on these points see: Molnar, A., Parsons, C. and Zouave, E. (2017). Computer Network Operations and Rule with Law in Australia, *Internet Policy Review, 6*(1). doi: 10.14763/2017.1.453

[48] Herpig, S. and Heumann, S. (2017, April 13). Germany's Crypto Past and Hacking Future. *Lawfare Blog*. Retrieved from https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future; Hughes, M. (2017,

Any move to weaken or undermine encryption systems must be differentiated from 'non-targeted' network-level measures and targeted access of 'end-points'. We insist that acquiring access to encrypted communications should occur without the wholesale weakening, circumvention, or undermining of the protection mechanism itself. While encryption may increase some degree of friction within a chain of criminal investigation, we suggest that there are many already existing technical and legal avenues for law enforcement to pursue without resorting to weakening, circumventing, or otherwise undermining encryption systems. Any attempt to do so overlooks the forensic value of already existing legal and technical capabilities, with great cost to the security and safety that encryption tools provide for individual ordinary citizens, consumers, businesses, and the government itself.

Big data and algorithmic policing

Big data policing is emerging with widespread information collection and implementation of data-led decision making and an intensification on prediction through algorithmic profiling in policing contexts.[49] This is closely associated with risk-based and pre-crime approaches.[50] These new data-driven approaches to policing present concerns for human and due process rights. For example, in a comprehensive empirical study of the structural and operational changes associated with the digitisation of policing in the Los Angeles Police Department (LAPD) a number of unintended consequences were identified including net-widening of the criminal justice dragnet in inequitable ways compounding discrimination and disadvantage, leading individuals to avoid contact with institutions that may 'surveil' them (for example social services).[51]

While big-data analytics and associated algorithmic decision-making have the potential to improve the efficiency and accuracy of government decision-making, they can also be used in ways that are harmful to individuals.[52] This may include pre-existing biases being built into algorithms that target 'risky' individuals or already marginalised groups.[53] The use of algorithms in criminal justice contexts has the potential to be especially problematic as it can involve targeting surveillance and policing activities, or increased monitoring on the basis of predicted risk (where risk predictions may be based on inaccurate administrative data or spurious relationships). These processes are not neutral, and there is the potential for bias and

July 28). Germany's police don't need backdoors because they can hack your phone anyway. *The Next Web*. Retrieved from https://thenextweb.com/insider/2017/07/28/germanys-police-dont-need-backdoors-because-they-can-hack-your-phone-anyway/?amp=1.

[49] Sanders, C. and Sheptycki, J. (2017). Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance. *Crime, Law and Social Change, 68*(1-2): 1-15. doi: 10.1007/s10611-016-9678-7; Ferguson, A. (2017). The Rise of Big Data Policing. New York University Press: New York.

[50] Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology, 11*(2), 261-281. doi: 10.1177/1362480607075851

[51] Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977-1008. doi: 10.1177/0003122417725865

[52] Bennett-Moses, L. and Chan, J. (2014). Using big data for legal and law enforcement decisions: Testing the new tools. *UNSW Law Journal. 37*(2), 643-678. Retrieved from https://ssrn.com/abstract=2513564; Bennett-Moses, L. and Chan, J. (2016). Algorithmic prediction in policing: Assumptions, evaluation and accountability, *Policing and Society,* 1-17. doi: 10.1080/10439463.2016.1253695.

[53] Friedman, B. and Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems, 14*(3), 330-347. doi: 10.1145/230538.230561

discrimination to become inscrutable and incontestable with increased barriers to transparency via a potentially false veil of objectivity provided by computerisation. These issues should also be considered in the context of the recent RoboDebt scandal where dataset validity and the impacts of error were also identified in the subsequent Senate inquiry into the procedural justice failures and general (mis-)management of the 'better management of the social welfare system initiative.'[54]

In striving for increased efficiency through automation, procedural and due process safeguards may be undercut. New forms of 'automatic justice' are challenging the traditional model of criminal justice where divisions between surveillance, adjudication and punishment are eroding with new forms of surveillance and automated decision-making that remove humans entirely.[55] Here, 'black-box' decision-making creates a lack of transparency in how policing decisions are being made by machines.

Accountability structures for big data policing and algorithmic decision-making in policing contexts should be implemented. There have been some attempts to regulate these developments in the European Union through the new General Data Protection Regulation, expected to come into force in early 2018. Aspects of the GDPR explicitly relate to automated decision-making, non-discrimination and a right to explanation for algorithmic decision-making.[56] Privacy, data protection, anti-discrimination, right to explanation, and review and appeal regulatory structures and policy frameworks should be considered in Australian contexts prior to implementation of big data policing and algorithmic profiling.

Biometrics, especially facial recognition

Facial recognition systems digitise, store and compare facial templates that measure the position of facial features and can be used to conduct one-to-one matching to verify identity, or one-to-many searching of databases to identify unknown persons. It provides a gateway connecting an individual's presence in physical space to information stored in large and ever-expanding databases held by government, law enforcement and security agencies (as discussed immediately above). Photographs (and facial templates) from data rich environments such as social media can be mined and integrated into big data. Face recognition can also be conducted from a distance and can be integrated with existing surveillance systems such as CCTV (known as 'Smart CCTV'), enabling tracking through public places.

In late 2015 the Commonwealth government announced a national facial recognition system - the National Facial Biometric Matching Capability or simply 'The Capability'- would be implemented. This occurred with absolutely no public consultation or public announcement at the time (it was only in late 2016 that The Capability attracted widespread media attention and public concern). This system uses existing identification documents, such as licences and passports, to extract and share biometric information between state, territory and national

[54] Community Affairs References Committee (2017). Senate inquiry into the design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative. Canberra: Commonwealth of Australia.

[55] Marks, A., Bowling, B. & Keenan, C. (2017). 'Automatic justice? Technology, crime and social control' (pp. 705-730). In R. Brownsword, E. Scotford & K. Yeung (Eds) *The Oxford Handbook of Law, Regulation and Technology*. Oxford: OUP.

[56] Goodman, B. & Flaxman, S. (2016). EU regulations on algorithmic decision-making and a "right to explanation. *ICML Workshop on Human Interpretability in Machine Learning.* New York: USA

government databases. Significantly, it was established through administrative processes and in a manner that does not require expanded police powers or the introduction of specific legislation.

Individuals who consented to providing a photograph to obtain a license or a passport did not consent to their facial templates being extracted from that image to be used for law enforcement, security, intelligence or other purposes. This is an example of function creep, where information collected for one purpose is used for secondary purposes beyond the scope or conditions supporting its original collection. This means information collected for one purpose can be used for, or integrated with, an infinite number of other unrelated purposes. The individual providing this information is not aware of, and thus has not consented to, these secondary or tertiary uses.

Under the *Privacy Act 1988* (Cth), sensitive information includes biometric information and templates. Sensitive information must only be collected with the consent of the individual concerned, unless the entity is an enforcement body and there is a reasonable belief that the information is necessary to the entity's functions. Entities cannot use or disclose information collected for a particular purpose for a secondary purpose without the consent of the individual, unless the information is reasonably necessary for one or more enforcement related activities. These exemptions are significant as enforcement agencies or agencies with an enforcement function do not need consent, a warrant, or a court order to collect and retain photographs, to process this information to create facial templates and disclose or share this information with other agencies.

Considerable developments have occurred in the roll out of national facial recognition systems and databases and urgent policy consideration is required to address legislative and regulatory shortcomings. The expansion of information collection and sharing by law enforcement and security agencies has not been matched with an expansion in oversight. A re-evaluation of privacy protections and the law enforcement exemptions in response to new technology is required, as are additional oversight mechanisms.[57]

6. Issues and concerns

In this section, we detail a number of overarching issues and concerns that relate to the points discussed above. Namely:

- There is limited empirical evidence surrounding the exact impacts of new ICTs on crime and policing. Legal and policing reforms and new measures concerning new technologies should be guided by robust evidence;
- There is no empirical evidence that supports the 'common-sense' assertion that blanket surveillance is effective at preventing serious crime and terrorism either domestically or internationally;
- The weak human rights protections in Australia mean that police have vast powers to intervene in the private lives of citizens. Australia has no comprehensive bill or constitutional protection of human rights and the limited protections that are available,

[57] Mann, M. and Smith, M. (2017). Automated facial recognition technology: Recent developments and strengthening oversight. *UNSW Law Journal, 40*(1), 121-145. Retrieved from http://unswlawjournal.unsw.edu.au/sites/default/files/04-mannsmith-advance-access-final.pdf

such as those provided by the *Privacy Act 1988* (Cth), are subject to significant law enforcement exemptions. In Australia, there are limited privacy protections relative to other all other liberal democracies[58] and current telecommunications interception and surveillance practices (such as mandatory metadata retention) are out of step with international precedent;

- Errors in police use of technology can lead to serious consequences for public safety. Examples include the Australian Federal Police (AFP) broadcast of its plans to arrest an alleged North Korean agent on social media or the continued operation of dark web sites as 'honeypots' or 'watering holes' by police that results in the continued downloading of images and repeat exploitation of victims, which has been recognised as a significant problem in the US *Playpen* investigation;
- The more that certain data is relied upon or fed into digital systems associated with law enforcement, the more likely certain populations or issues are disproportionately targeted or profiled, this is especially relevant to racial discrimination and bias and the disproportionate representation of Indigenous populations in the criminal justice system[59];
- Insufficient checks and balances as evidenced by the Australian Federal Police (AFP) accessing a journalists' metadata without warrant. The expansion of data collection and information sharing by law enforcement and security agencies has not been matched with an expansion in independent oversight of policing activity.

7. Recommendations

In this section, we outline our main recommendations as regards to the impacts of new ICTs and law enforcement, which aim to address existing regulatory gaps by placing *reasonable* limits on police conduct:

1. As a matter of international comity, follow international precedent in surveillance programs and practices (for example mandatory metadata retention) and with regard to, and respect of, international human rights standards;
2. Suspend the current program of mandatory data retention and require a judicial warrant to access telecommunications information;
3. Do not implement law or practices that involve undermining or weakening encrypted forms of communication and make use of existing targeted powers for accessing telecommunications information (via a judicial warrant as per the recommendation immediately above);
4. In the case of investigations with an extraterritorial element there must be recognition that Australian police and data analysis procedures comply with established MLAT procedures. If streamlined bi- or multi-lateral procedures are to be developed, ensure domestic legislation:

[58] Williams, G. and Reynold, D. (2017). A charter of rights for Australia. Melbourne: MUP.

[59] Warren, I., Lippert, R., Walby, K. and Palmer, D. (2013). When the profile becomes the population: Examining privacy governance and road traffic control in Canada and Australia. *Current Issues in Criminal Justice 25*(2), 565-584. Retrieved from https://www.researchgate.net/profile/Ian_Warren2/publication/259324842_When_the_Profile_Becomes_the_Population_Examining_Privacy_Governance_and_Road_Traffic_Surveillance_in_Canada_and_Australia/links/5668fb9d08ae193b5fa13d3f/When-the-Profile-Becomes-the-Population-Examining-Privacy-Governance-and-Road-Traffic-Surveillance-in-Canada-and-Australia.pdf

   a. reflects the need for compliance with the jurisdictional and sovereign interests of other nations where data or suspects might be located as recognised under international law;
   b. reinforces the need for warrant requirements and principles governing the admissibility of evidence to protect the due process rights of crime suspects and enhance the legitimacy of online investigative techniques;
   c. reinforces the need for clear protocols and independent oversight of special investigations, including the seizure and operation of offshore websites by Australian law enforcement agencies;
5. Where transnational cooperation is sought, the burden of responsibility for instigating and complying with requests rests with law enforcement agencies. Hence, to ensure both the admissibility of evidence and the integrity of transnational investigations, it is necessary to:
   a. obtain written records demonstrating consent has been obtained from foreign law enforcement or government agencies, and these requirements are reciprocal based on the geographic location of the data, the website and/or suspect being investigated;
   b. that legal standards for obtaining these records be established based on sufficient proof at the pre-trial standard of reasonable suspicion;
   c. that the collection of evidence through CNO/NIT techniques be strictly monitored by an external agency, to limit the geographic scope, reach, scale and time frame for collecting relevant evidence;
   d. where additional data is required from offshore ISPs or government agencies, there is a trail of correspondence documenting the nature of the request, the evidence subject to exchange and the ISP or government agency's response;
   e. these requirements should also determine the admissibility of extraterritorial evidence during pre-trial or trial procedures; and
   f. where requests are made to or received from jurisdictions where English is not the first language, appropriate paperwork and training on these reciprocal procedures to ensure compliance with local evidentiary and language requirements in the foreign jurisdiction.
6. Implement appropriate and robust oversight structures for police use of new ICTs;
7. Gather robust independent evidence on which reforms to law and policing on the basis of new technologies are guided and based;
8. Increased government funding for independent research in the topics outlined above.
   a. Criminology research funding is limited (the Criminology Research Council awards have not been opened in the previous year, and there has been speculation that they will be only be open for application in some research areas only). We therefore recommend that future awards be targeted at the impacts of ICTs on law enforcement and that the Criminology Research Advisory Council prioritise funding applications in this area.

8. About

Authors

Dr Monique Mann is the Vice Chancellor's Research Fellow in Technology and Regulation at the Faculty of Law, QUT. Dr Mann is advancing a program of socio-legal research on the privacy and human rights implications police technology and transnational online policing. She is on the Board of Directors and Co-Chair of the Surveillance Committee of the Australian Privacy Foundation and the Advisory Council of Digital Rights Watch Australia.

Dr Adam Molnar is a Lecturer in Criminology at Deakin University. His research examines socio-legal aspects of surveillance technologies, with a particular focus on practices of security intelligence and law enforcement. He is Vice-Chair of the Australian Privacy Foundation, Co-Chair of the Surveillance Committee of the Australian Privacy Foundation, and on the Advisory Council of Digital Rights Watch Australia.

Dr Ian Warren is a Senior Lecturer in Criminology at Deakin University, who has widely written in Australian and international journals on issues relating to transnational crime, criminal law and policing jurisdiction. He is a member of the Australian Privacy Foundation and on the editorial board of the Australian and New Zealand Journal of Criminology.

Dr Angela Daly is Vice Chancellor's Senior Research Fellow in QUT Faculty of Law and research associate in the Tilburg Institute for Law, Technology and Society (Netherlands). She is a socio-legal scholar of the regulation of new technologies and is the author of *Socio-Legal Aspects of the 3D Printing Revolution* (Palgrave 2016) and *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016). She is also a Director of Digital Rights Watch Australia.

Organisations

The Australian Privacy Foundation is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Digital Rights Watch Australia is a charity organisation founded in 2016 whose mission is to ensure that Australian citizens are equipped, empowered and enabled to uphold their digital rights.

Future Wise is an independent policy and advocacy organisation, which focuses on the interactions between technology, healthcare, education and their effects on society.

Electronic Frontiers Australia Inc. is a non-profit national organisation that has been promoting and protecting digital rights (civil liberties) in Australia since it was established in January 1994.

8. Bibliography of author works in ICTs and law enforcement

Daly, A. (2016). *Socio-Legal Aspects of the 3D Printing Revolution*. UK: Palgrave Macmillan.

James, S. and **Warren, I.** (2010). Australian police responses to transnational crime and terrorism. In D. Das and J. Eterno (Eds.), *Police Practices in Global Perspective* (pp. 131-172), Lanham MD: Rowman and Littlefield.

Kennedy, S. and **Warren, I.** (forthcoming). Southern criminology, law and the 'right' to consular notification in Australia, New Zealand and the United States. *International Journal For Crime, Justice And Social Democracy* (accepted for publication 2 Feb 2018).

Lippert, R., Walby, K., **Warren, I.** and Palmer, D. (2016). *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective*. UK: Palgrave Macmillan.

Mann, M. (2016, October 11). Worried your emails might be spied on? Here's what you can do. *The Conversation.* Retrieved from https://theconversation.com/worried-your-emails-might-be-spied-on-heres-what-you-can-do-66574

Mann, M. and Smith, M. (2017). Automated facial recognition technology: Recent developments and strengthening oversight. *UNSW Law Journal, 40*(1), 121-145. Retrieved from http://www.austlii.edu.au/au/journals/UNSWLJ/2017/6.html

Mann, M. (2017, April 7). The Capability: Facial Recognition, privacy and regulating new technology. *Australian Security Magazine.* Retrieved from https://issuu.com/apsm/docs/asm_april_may_final

Mann, M. (2017, July 11). The RoboCop continuum: Confronting automated and robotic policing. *Australian Security Magazine.* Retrieved from https://issuu.com/apsm/docs/asm_june_july_2017

Mann, M., Daly, A., Wilson, M. and Suzor, N. (forthcoming, 2018). The limits of (digital) constitutionalism? Exploring the privacy-security (im)balance in Australia. *International Communication Gazette* (accepted for publication, September 2017).

Mann, M., Molnar, A. & Warren, I. (2017, July 21). Spyware merchants: Outsourcing government hacking and digital forensics. *The Conversation*. Retrieved from https://theconversation.com/spyware-merchants-the-risks-of-outsourcing-government-hacking-80891

Mann, M. and Warren, I. (2018). The digital and legal divide: *Silk Road*, transnational online policing and Southern criminology. In K. Carrington, R. Hogg, J. Scott and M. Sozzo (Eds.) *The Palgrave Handbook of Criminology and the Global South* (pp. 245-260), Springer: Cham, Switzerland.

Mann, M., Warren, I. and Kennedy, S. (forthcoming, 2018). The legal geographies of transnational cyber-prosecutions: Extradition, human rights and forum shifting. *Global Crime* (accepted for publication, November 2017)

Mann, M. and Wilson, M. (2016, July 28). As surveillance gets smart, hackers get smarter. *The Conversation.* Retrieved from https://theconversation.com/as-surveillance-gets-smart-hackers-get-smarter-62773

Molnar, A., Parsons, C., & Zouave, E. (2017). Computer network operations and 'rule-with-law' in Australia. *Internet policy review*, *6*(1), 1-14. doi: 10.14763/2017.1.453

Molnar, A. (2017). Technology, Law, and the Formation of (Il)Liberal Democracy?. *Surveillance & Society*, *15*(3/4), 381. doi: 10.1080/13510347.2013.851672

Palmer, D. and **Warren, I.** (2013). Global Policing and the Case of Kim Dotcom. *International Journal For Crime, Justice And Social Democracy, 2*(3), 105-119. doi: 10.5204/ijcjsd.v2i3.105

Palmer, D., **Warren, I.** and Miller, P. (2013). ID-scanners in the night-time economy: Social sorting or social order? *Trends and Issues in Crime and Criminal Justice no. 466*. Canberra: Australian Institute of Criminology. Retrieved from http://www.aic.gov.au/publications/current%20series/tandi/461-480/tandi466.html

Smith, M., **Mann, M.,** and Urbas, G. (2018). *Biometrics, Crime and Security.* UK: Routledge.

Warren, I. (2015). Surveillance, criminal law and sovereignty. *Surveillance and Society 13*(2), 300-305. Retrieved from https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/law_sovereign/law_sov.

Warren, I. and Palmer D. (2015). *Global Criminology*. Pyrmont NSW: Thomson Reuters/Law Book Company, 272-274.

Warren, I., Lippert, R., Walby, K. and Palmer, D. (2013). When the profile becomes the population: Examining privacy governance and road traffic control in Canada and Australia. *Current Issues in Criminal Justice 25*(2), 565-584.

Warren, I., Molnar, A. and **Mann, M.** (2017, September 7). Poisoned water holes: The legal dangers of dark web policing. *The Conversation*. Retrieved from https://theconversation.com/poisoned-water-holes-the-legal-dangers-of-dark-web-policing-82833

Wilson, M. and **Mann, M.** (2017, September 8). Police want to read encrypted messages, but they already have significant power to access our data. *The Conversation.* Retrieved from https://theconversation.com/police-want-to-read-encrypted-messages-but-they-already-have-significant-power-to-access-our-data-82891