LECC
Law Enforcement
Conduct Commission

Phone: 02 9321 6700 Fax: 02 9321 6799
Level 3, 111 Elizabeth Street, Sydney NSW 2000
Postal address: GPO Box 3880, Sydney NSW 2001
www.lecc.nsw.gov.au

40190/10

29 January 2019

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Committee Secretary,

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

Thank you for the opportunity to provide a further submission to the Committee.

On 9 October 2018, the Law Enforcement Conduct Commission provided a submission to the Committee in response to the review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ("The Bill").

The initial submission which expressed the LECC's views regarding the bill are maintained and also are relevant to the review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ("the Act"). I therefore annexe the LECC's initial submission for the Committee's consideration within the review of the Act.

The key points from the initial submission were-

1. The LECC is a statutory agency established under section 17 of the *Law Enforcement Conduct Commission Act 2016* (NSW) for the investigation and oversight of law enforcement misconduct in New South Wales (NSW).
2. The LECC relies significantly on telecommunications interception warrants to investigate serious offences allegedly committed by New South Wales Police Force (NSWPF) officers.
3. The prevalence of encrypted content collected under such warrants has risen significantly over the last five years. In 2018, 93% of IP communications intercepted by virtue of LECC warrants were encrypted.
4. The LECC's digital forensics capability is also hindered by the use of encryption to secure devices and digital storage.
5. The legislative access to "designated communications providers" provided within Schedule 1 of the Act would assist the LECC's investigation of serious offences.

In addition to the initial LECC submission, I request that the Committee consider the additional points raised within this submission.

The LECC's Exclusion from Schedule 1 Powers

The Bill was drafted to grant Schedule 1 Powers to all interception agencies. The Committee's Advisory Report on the Bill recommended (Recommendation 3) that the LECC, as a "State and Territory independent commissions against corruption", should be excluded from the scope of Schedule 1. The rationale behind this recommendation is not stated in the Report and is otherwise unexplained.

The Act allows police to use Schedule 1 powers to investigate "prescribed offences" as defined by the *Telecommunications (Interception and Access) Act 1979*. Prescribed offences include all offences which attract a penalty of at least three years imprisonment. The Act does not, however, enable the LECC to use Schedule 1 powers to investigate prescribed (or even serious) offences committed by police officers.

The Need for Effective Investigations into Police Corruption

Police are provided with a wide array of powers including the ability to detain, search, arrest, use force, enter private premises and seize property, engage in covert investigations and surveillance. Due to these extensive and often invasive powers, the need for vigorous oversight mechanisms is evident and has been demonstrated by a number of Royal Commissions. Elements that allow for an effective oversight mechanism must include the power and capacity to conduct independent investigations and access to a variety of covert and surveillance techniques. Particularly as the nature of crime and misconduct expands to include methods enabled by technological advances, such as encryption tools, law enforcement agencies, including the LECC, must also expand their powers to combat this activity effectively.

Corruption and misconduct of police officers compromises the confidence the public have in the fairness, integrity and honesty of all police officers, not merely those in state police forces. Corruption in the NSWPF diverts resources from providing its core business and services to the community. Mistrust of police has detrimental effects on policing as public involvement is a crucial element of law enforcement, as police often need members of the public to report and assist with information. A lack of trust also adversely effects the effectiveness of policing in the community, and decreasing the credibility of police officers as witnesses leading to negativity and a lack of confidence in the criminal justice system. As such, corruption in the police force strikes at the heart of community safety and the justice system. The independent, external investigations conducted by the LECC are vitally important for the efficacy of the police accountability system. Not only do these investigations directly reduce corrupt activity within the NSWPF, they also act as a deterrent. Knowledge or suspicion that the LECC has covert capability is significant in this respect.

The New South Wales Police Force is the largest in Australia with 20,725 members, 16,788 sworn officers and 3,937 unsworn officers. It serves more than 7.9 million people, approximately 32% of Australia's total population.[1]

[1] 2017-2018 NSW Police Annual Report 2018, Office of the Commissioner,

The Use of Encryption to Enable Corruption

Emerging technology, whilst providing many benefits, is changing criminality. The Australian National Cyber Security Strategy noted that there is a "growing trend for groups and individuals to use encryption to hide illegal activity and motivate others to join their cause"[2]. The Act provides some law enforcement agencies with powers to keep up with these changing technologies.

The investigation of criminal activity conducted by police is, in many instances, more challenging than for other criminals. Police are well versed in investigative methods, tools and surveillance techniques. They also have access to intelligence databases and other sources of intelligence such as human sources. In particular, police are aware of the sensitive capabilities involving electronic collection. Interception operations conducted under LECC warrants show that police targets currently use encryption to facilitate criminal activity.

The exclusion of the LECC within Schedule 1 of the Act may well encourage corrupt police to use encrypted communications with confidence and encourage police corruption more broadly.

As part of this review, I request that the Committee reconsider the LECC's inclusion within Schedule 1 powers of the Act, as was intended by the Bill.

[redacted]

The Hon M F Adams QC
Chief Commissioner

[2] Department of the Prime Minister, Commonwealth of Australia (2106) *Australia's Cyber Security Strategy,* <https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf>

LECC
Law Enforcement
Conduct Commission

Submission to the Parliamentary Joint Committee for Intelligence and Security

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill

The Law Enforcement Conduct Commission

The Law Enforcement Conduct Commission (LECC) is a statutory agency established under section 17 of the *Law Enforcement Conduct Commission Act 2016* (NSW) for the oversight of law enforcement in New South Wales (NSW). The LECC commenced operations on 1 July 2017 and replaced the Police Integrity Commission (PIC), the Police Compliance Branch of the NSW Ombudsman's office and the Inspector of the Crime Commission.

In light of the PIC's transition into the LECC and for the purposes of this submission, the PIC and the LECC will henceforth be referred to as "the Commission".

The Commission is an independent body exercising royal commission powers to detect, investigate and expose misconduct and maladministration within the NSW Police Force (NSWPF) and the NSW Crime Commission (NSWCC). The Commission also has the power to independently oversight and monitor the investigation of critical incidents by the NSWPF if it decides that it is in the public interest to do so. Furthermore, the Commission oversees NSWPF and NSWCC investigations of alleged misconduct by officers of those agencies.

The Commonwealth Attorney General has declared the Commission to be an "Agency" for the purposes of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) allowing it to apply for, and be issued, telecommunications interception warrants. The commission operates equipment to facilitate the lawful interception of communications by virtue of such warrants.

The Impact of Encryption on Telecommunications Interception Conducted by the Commission

Telecommunications interception is a cost-effective and powerful tool reserved for the investigation of serious criminal offences. The interception of communications under warrant has enabled the Commission to collect vital, and often compelling, evidence used within hearings and prosecutions. In addition, the Commission has regularly disclosed lawfully intercepted information to the NSWPF to assist in the management of the officers implicated in misconduct.

The Commission was issued with 162 telecommunications interception warrants over the last five years as indicated in the table below.

Financial Year	Telecommunications Interception Warrants issued
2013 - 2014	35
2014 - 2015	48
2015 - 2016	60
2016 - 2017	2
2017 - 2018	17
Total	**162**

Table 1: Telecommunications interception warrants issued by financial year.

The application of interception powers permits the collection of communications in various categories such as telephone calls, text messages, messaging applications, emails, social media, chat sessions, and other online activity. Changes in communication technologies have caused two significant changes within the lawful interception environment:

1. The migration of communications from traditional telephone calls and text messages to Internet Protocol (IP) based communications; and
2. The increased proportion of IP based communications being encrypted.

Whilst the majority of telephone calls and text messages remain unencrypted and intelligible to agencies, the vast majority of IP based communications are now encrypted by default (this includes messaging applications, email, and social media). The Commission is technically unable to decrypt these communications.

It is a well-known fact that in society's rapidly changing technological landscape, encryption of communications has increased and continues to rise. "Rapid developments in communications technology present both opportunities and challenges for our agencies," former Prime Minister Malcom Turnbull said in a national security statement delivered in the wake of terrorist attacks in Paris.[1]

Encryption presents challenges for Australian law enforcement and security agencies in continuing to access data essential for investigations to keep all Australians safe and secure. The Commission supports privacy principles and encourages people to take measures to protect their own privacy generally. However, for the investigation of serious criminal offences, the Commission depends on Telecommunications Interception as a primary tool in investigations for the collection of evidence.

The deployment of telecommunications interception and surveillance devices by law enforcement agencies, including the Commission, yields high returns in evidence collection. There are, however, significant gaps in collection which can be easily exploited by the Commission's targets to conduct corrupt activity. Australia's national cyber security strategy, launched in April 2016, noted that there is "*a growing trend for groups and individuals to use encryption to hide illegal activity and motivate others to join their cause*". Police targets, in particular, will modify their activities to avoid interception as they are well versed in law enforcement methods.

Resultantly, the evidentiary value of Telecommunications Interception material has diminished over the last decade with the rise of encrypted social media and messaging applications.

An Analysis of IP Based Communications Intercepted under Commission Warrants

The statistics in this section have been extracted directly from the Commission's Telecommunications Interception System.

In the current electronic communications environment, there are many mainstream and encrypted alternatives to traditional voice or SMS communication. There has been an

[1] Pearce, Rohan 2015, 'Encrypted comms present a challenge for ASIO, Turnbull says', *Computerworld*, https://www.computerworld.com.au/article/589586/encrypted-comms-present-challenge-asio-turnbull-says/

evident rise on Commission intercepts of targets using voice and messaging applications which have end-to-end encryption. Some of these applications are illustrated below.

Figure 1: Examples of encrypted communications detected on Commission intercepts.

The trend line within figure 2 below illustrates the gradual increase of encrypted IP sessions intercepted by the Commission each year, rising to over 90 per cent in the last 18 months.

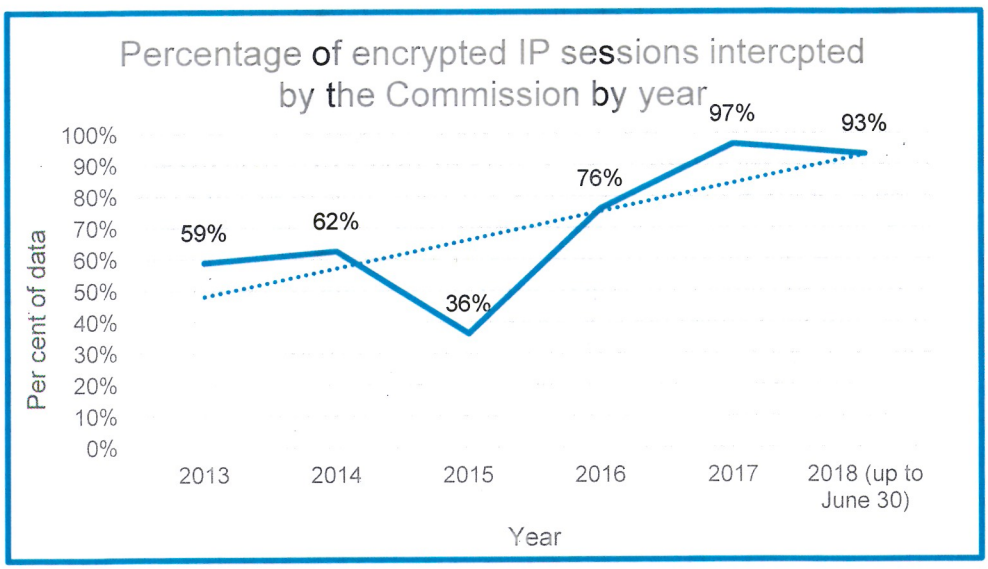

Figure 2: The percentage of encrypted IP sessions intercepted under warrant by the Commission by year.

The following figure 3 demonstrates the current encryption landscape. It illustrates how the vast majority of IP data intercepted under warrants by the Commission in 2018 is encrypted.

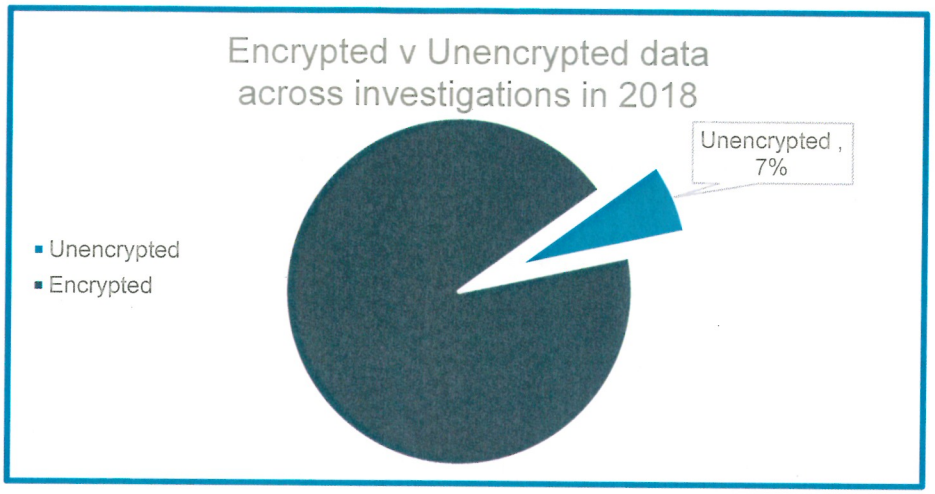

Figure 3: The proportion of encrypted and unencrypted IP sessions intercepted by the Commission in 2018.

The Commission's targets make considerable use of encrypted communications. A statistical analysis of interception activity on a recent investigation provides an example of the extent of encryption encountered in the current communications environment. In this Operation, 94 per cent of communications were encrypted.

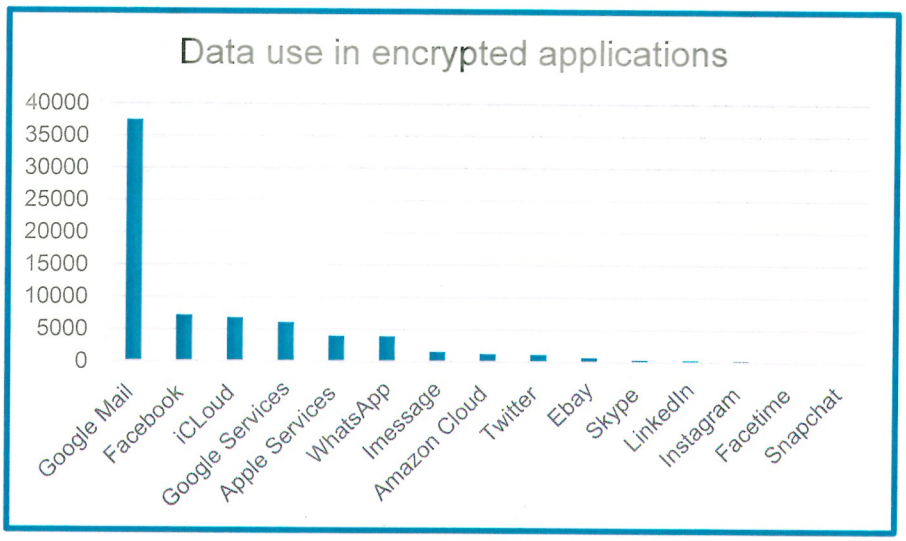

Figure 4: Encrypted sessions is by Commission targets in a recent investigation.

Figure 4 illustrates the vast array of encrypted applications that were used as a means of communication between Operation targets. It also shows the number of encrypted sessions from well-known applications that were used by the targets within this Operation. In this case, 15 different applications were used to varying degrees.

The communication providers depicted in figure 4 are likely being used by Commission targets to further criminal activity in Australia. Commission targets are police officers or persons facilitating misconduct by police. The communication providers are based overseas and are not subject to Australian interception laws.

The Impact of Encryption on Digital Forensic Examinations Conducted by the Commission

Another important tool in modern investigations is digital forensics. In many instances digital evidence obtained from computers, smart phones, storage devices and other equipment provides direct evidence in support of criminal investigations.

The Commission maintains a contemporary digital forensics capability which includes a dedicated lab, systems and equipment. The extraction of digital evidence from networks, hard drives and smartphones etc can also be defeated by encryption. Certain applications and operating systems can partially or fully encrypt the storage component, or the entire device being examined.

Currently, the Commission's Digital Forensic capabilities are not hindered to the same extent by encryption as with interception. However, it is anticipated that the use of encryption to secure devices and digital storage will increase as time goes on. A legal framework to request technical assistance from technology providers for the investigation of criminal offences could greatly assist on a case-by-case basis.

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – Schedule 1

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (the Bill) proposes to provide interception agencies with lawful avenues to seek or require assistance from communication providers operating in Australia.

The Commission supports the proposed changes within Schedule 1 and makes the following comment.

It is the view of the Commission that the proposed changes in Schedule 1 will not result in comprehensive decryption of intercept product. Although, defining Designated Communication Providers (DCPs) (s317C) in addition to "listed acts or things" (s317E), is a significant legislative change which will allow lawful avenues for the Commission to seek assistance in particular circumstances.

It is important to note that the Bill does not propose to extend the jurisdiction of Australian interception warrants to DCPs. Any further assistance relating to encrypted content provided under Schedule 1 would be for content already lawfully obtained by the Commission.

It is the Commission's view that proposed definitions for DCPs and "listed acts or things" provides for practical avenues to request assistance in support of both interception and digital forensics operations.

It is also the Commission's view that the practical application of assistance through Technical Assistance Requests (s317G), Technical Assistance Notices (s317L) and Technical Capability Notices (s317T) provide a flexible and graduated framework depending on the type of assistance sought.

In many cases the Commission may seek technical advice relating to devices or services only, and this particularly relates to digital forensics. This advice would be practically

requested through a Technical Assistance Request. This procedure seems reasonable and efficient.

A Technical Assistance Notice is a compulsory order to the DCP. This provides an effective method for the Commission to gain assistance. It is noted that this assistance will not extend behind the current capability of the provider. To issue a Technical Assistance Notice under s317P the Chief Officer must be satisfied that the requirements imposed by the notice are reasonable and proportionate, and compliance with the notice is practicable and technically feasible. The Commission believes this is a fair and rational test where a two-step process provides a strong safeguard against technical assistance requests that are unduly burdensome on telecommunication providers.

The Chief Officer's satisfaction of reasonableness and proportionality must be formed on a correct understanding of the law, and must not take into account a consideration which a court can determine in retrospect 'to be extraneous to any objects the legislature could have had in view'. Given the Chief Officer of the Commission is a former Supreme Court judge who would be very familiar with the application of such a test, the parliamentary committee can be assured that requests would not be considered lightly and there are strong protections in place to ensure that interception powers are exercised as intended.

The following case study is a real example of how the proposed changes in Schedule 1 would have assisted the Commission recently.

Case Study

In April 2016 the Commission received a number of complaints, which alleged that NSW Police officers created, shared and engaged with offensive material targeted at a NSW Member of Parliament (NSW MP). In response to these complaints, the Commission established Operation Colchester.

The investigation found evidence which indicated that racist, sexist and abusive comments were made about the NSW MP through personal Facebook accounts of serving NSW Police officers. Attempts were made by the Commission to obtain IP addresses directly from Facebook in order to identify who operated the Facebook accounts.

An initial request for information citing the relevant sections of the TIA Act was made to Facebook in April 2016. At this time it was also observed that Facebook would keep information for 90 days if a person deletes their account. This response was rejected due to insufficient information, however Facebook did note that one of the target's accounts had been deleted.

A second request was made to Facebook in May 2016 which Facebook took one month to respond to and was also rejected. Facebook instead requested a Mutual Legal Assistance Treaty (MLAT) request in order to be able to assist. The commission made this request but by late August was unable to gather this evidence. A decision was made to go to the Commonwealth Department of Public Prosecution (CDPP) as there were concerns that waiting for the MLAT process to complete would not allow a timely investigation.

The Commission sought advice from the CDPP as to whether two officers could be prosecuted for their Facebook posts pursuant to section 474.17 of the *Criminal Code 1995*

(Cth). The CDPP advised that there was insufficient evidence to prosecute either of the officers and cited the lack of identifying IP addresses is an important evidentiary deficiency.

As Facebook was based offshore, the Commission had no way of compelling the production of information it was seeking.

Within the proposed amendments, the designation of Facebook is a DCP and the lawful avenues of both technical assistance requests and technical assistance notices would have provided the commission with practical and lawful ways to gather this evidence in support of a prosecution.

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – Schedule 2 - 5

The proposed amendments in Schedule 2 - 5 relate to Commonwealth law and are very unlikely to be used by the Commission. The Commission does support the changes in principle however, and makes the following comments.

The proposed amendments in Schedule 1 will assist the Commission. It should be recognised, however, that these additional powers will not provide a holistic solution to encrypted, intercepted material. In combination with the amendments in Schedule 1, proposed amendments in Schedules 2 and 3 provide other practical avenues to gather evidence within the current technological landscape.

The proposed amendments to the *Surveillance Devices Act 2004,* will assist, agencies obtain evidence through surveillance device warrants as opposed to interception warrants. By doing so an alternate means to collection pre or post encryption is possible.

The inclusion of a Computer Access Warrant in Schedule 2, is a potential avenue to collect evidence which is encrypted in transit.

The definitions and legal avenues concerning "account-based data" in Schedule 3 also provide practical means to gather digital evidence under a search warrant. In the modern technological environment, an individual's data is no longer stored purely on devices seized within search warrants. It is likely that the storage of incriminating information would be well hidden via encryption or an online location. This is similar to methods used within criminal activity where incriminating physical evidence is hidden to avoid detection by law enforcement agencies.

Conclusion

The Commissions ability to gather evidence relating to police misconduct or corrupt activity is being diminished through advances in communications technology.

The migration of communications from traditional voice and text to IP-based communications combined with the proportion of these communications being encrypted is having a real and measurable impact on traditional methods to gather evidence such as telecommunications interception. In addition, the wide choice of encrypted communication options from overseas providers allows for easy access to secure

communications to conduct criminal activity.

The Commission fully supports the amendments proposed within the Bill.

It is understandable that the Australian community may hold concerns when granting further powers to law enforcement agencies. It should be noted that these powers are reserved for targeted assistance relating to criminal activity and do not allow for widespread collection of innocent parties.

The Commission supports the proposed amendments as it will greatly assist in the investigation of misconduct by police. Whilst the Bill does provide additional powers to police, it also provides additional powers to oversight bodies like the Commission to assist in the investigation of police where they misuse their powers or engage in criminal or corrupt activity.