LECC
Law Enforcement
Conduct Commission

Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

The Law Enforcement Conduct Commission

The Law Enforcement Conduct Commision (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 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). Furthermore, the LECC oversees the NSWPF and NSWCC investigations of alleged misconduct by officers of those agencies.

The LECC is delcared 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 LECC is also a declared "Criminal Law Enforcement Agency" for the purpose of the TIA Act allowing it to apply for and be issued with stored communcation warrants, as well as allowing it access telecommunicaitons data in support of criminal investigations.

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 transition from the PIC into the LECC, the references to 'the LECC' within this submission shall henceforth refer to both agencies.

The LECC would like to thank the Committee for the opportunity to present the following submision in relation its review of the Telecommunications Legislaiton Amendment (International Produciton Orders) Bill 2020 ('the Bill').

The LECC's Support of the Bill

The LECC supports the Bill as it mitigates the degredation of existing investigative capabilities.

The TIA Act provides interception agencies powers to collect evidence by virtue of telecommunications interception warrants, stored communications warrants and via access to telecommunications data. These are effective investigative tools which the LECC relies heavily upon for the investigation of serious criminal offences.

In many cases, communications used to facilitate criminal activity have migrated from traditional telecommunications services provided by Australian carriers, to new services provided internationally based designated communication providers (DCPs). These communications can be lawfully intercepted under Australian warrants (served on Australian carriers), however, in most cases the content is encrypted by the DCP.

The Bill will provide a lawful avenue for Australian agencies to collect this evidence way of internetional production orders (IPOs). This is consistent with the authority provided under exisiting warrants and historical collection capabilities.

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 over the top (OTT) and social media communication services, 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. 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. 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 compromises 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 21,080 members, 17,111 sworn officers and 3,969 unsworn officers. It serves more than 8 million people, approximately 32% of Australia's total population. [1] It is vital that a police force of this size is providedwith effective oversight.

The Investigation of Serious Offences by the LECC

Over the last two years the LECC has investigated serious offences including, trafficking a controlled drug – s302.4(1) of the *Criminal Code Act 1995* (Cth), fraud - s192E(1) of the *Crimes Act 1900* (NSW), supply of a prohibited drug – s25(1) of *Drug Misuse and Trafficking Act 1985* and bribery and corruption s200(2) of the *Police Act 1990* (NSW).

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 LECC to collect vital, and often compelling, evidence used within hearings and prosecutions. In addition, the LECC has regularly disclosed lawfully intercepted information to the NSWPF to assist in the management of the officers implicated in misconduct.

The LECC was issued with 180 telecommunications interception warrants and 34 stored communications warrants for the investigation of serious offences over the last six years as indicated in the table below.

Financial Year	Telecommunications Interception Warrants Issued	Stored Communications Warrants Issued
2013 – 2014*	35	4
2014 – 2015*	48	7
2015 – 2016*	60	16
2016 - 2017	2	1
2017 - 2018	17	1
2018 - 2019	18	5
Total	180	34

Table 1: Telecommunications interception and stored communications warrants issued by financial year. *Warrants sought by the PIC.

[1] 2018-2019 NSW Police Annual Report 2019, Office of the Commissioner.

The nominated offences listed on each of the warrants in Table 1 are category 1 serious offences or category 2 serious offences as prescribed by the Bill and would therefore meet the threshold for the application of an IPO if those powers were available at the time.

Degradation of Interception Effectiveness

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

1. The migration of communications from traditional methods provided by Australian carriers to an array of communication services provided by international DCPs and;
2. The increased proportion of communication services provided by DCPs being encrypted.

Due to the social and criminal uptake of communication technologies, the LECCs ability to gather evidence relating to criminal and corrupt activity is being diminished. The wide choice of encrypted communication options from international DCPs allows for easy access to secure communications to conduct criminal activity.

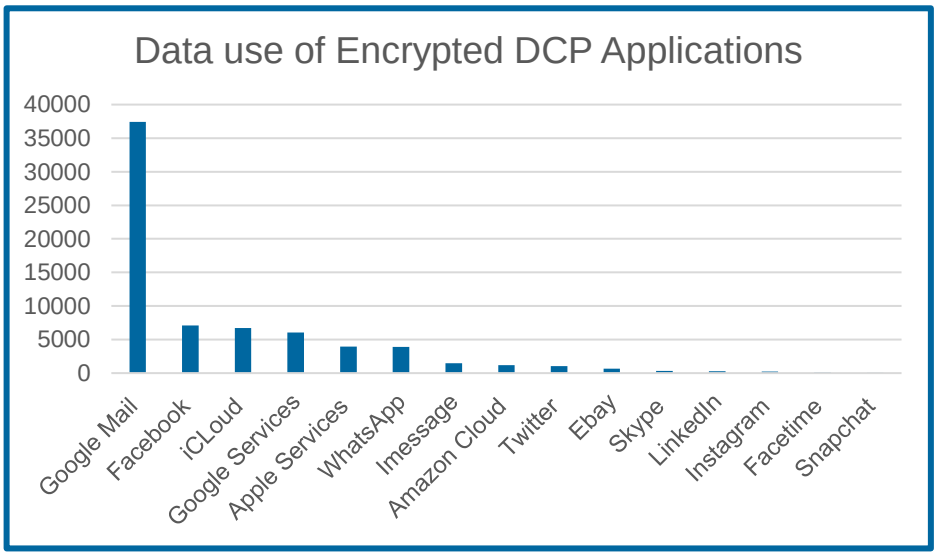

Figure 1: Encrypted DCP sessions used by LECC targets in a recent investigation.

The data from the Figure 1 was extracted from an interception from a recent investigation. In this investigation, the targets were police officers and persons facilitating misconduct by police. In many instances, LECC targets are well versed in interception capabilities available to law enforcement agencies. Given this, they are likely to use DCPs such as the ones depicted in Figure 1 in order to further criminal activities with the knowledge that these providers are based overseas and are not subject to the Australian interception warrant regime.

It is also important to note that the interception of this content is currently lawful in Australia under telecommunication interception warrants served on Australian carriers. Whilst the content provided by international DCPs traverses across Australian carrier networks, it is in an encrypted form when intercepted. The collection of this evidence in an intelligible form would be possible through an IPO.

Case Study

In April 2016 the LECC 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 LECC 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. Important identification evidence linking alleged suspects to the Facebook accounts was sought both directly from Facebook and through the Mutual Legal Assistance Treaty (MLAT). The suspected account was deleted which caused Facebook to delete this data after 90 days. Due to the inefficient and timely MLAT process, the identification evidence was not provided within the 90day deletion period.

The LECC sought advice from the Commonwealth Department of Public Prosecution (CDPP) as to whether two officers could be prosecuted for their Facebook posts pursuant to section 474.17 of the *Criminal Code 1995* (Cth) – using a carriage service to menace, harass or cause offence. The CDPP advised that there was insufficient evidence to prosecute either of the officers and cited the lack of identifying IP addresses as an important evidentiary deficiency.

Under arrangements proposed by the Bill, the LECC would have been able to apply for an IPO and, if issued, would have been able to lawfully serve it on Facebook to produce the required IP address.

Compliance and Oversight

The TIA Act provides a comprehensive compliance regime that applies to the collection, use and disclosure of content and data. In addition, the TIA Act in combination with various state legislation, prescribes a rigorous and independent oversight regime. Compliance and oversight requirements for interception, stored communications and telecommunications data is complex, robust and well understood by agencies and oversight bodies. The Bill leverages off this established compliance regime to apply consistency and rigour in the compliance and oversight of IPOs. The LECC believes this is an effective approach to ensure that evidence is collected and used lawfully whilst ensuring the privacy of non-targeted Australians.

Conclusion

The amendments proposed by the International Production Order Bill provide an effectve process and structure to support the investigation of serious offences. The ability to serve IPOs on international DCPs provides an avenue to collect evidence that is no longer possible under Australian interception warrants. The compliance and oversight measures are rigorous and consistent with the current TIA Act requirements and therefore effective.

The LECC also supports the reciprocal arrangements where our international partners are able to collect evidence in the event their citizens are suspected of using Australian DCP's to conduct serious criminal offences.