Submission No 192

Inquiry into potential reforms of National Security Legislation

Name: S Clancy
Assistant Director
Office of the CEO

Organisation: Australian Competition &
Consumer Commission
Marcus Clarke Street Canberra ACT 2601

Australian
Competition &
Consumer
Commission

Submission to the Parliamentary Joint Committee on Intelligence and Security

Inquiry into potential reform of national security legislation

August 2012

Summary and recommendations

The Australian Competition and Consumer Commission (ACCC) notes that the Committee has been asked to examine a wide array of reforms relating to national security, including proposals for telecommunications interception reform. The ACCC's submissions are limited to the issue of amendments which might be appropriate to the law enforcement provisions of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and what features of the existing regime should be retained into the future. In that context:

- The ACCC is strongly of the view that any change to the TIA Act should not reduce its capacity to effectively perform its functions.
- Privacy should remain a key theme in any new regime governing access to communications by law enforcement.

Communications information and data retention (TOR 2.a., 15.c.)

The ACCC recommends that the Committee recognise the benefit of communications information to the law enforcement activities of the ACCC. To ensure the continued capacity of the ACCC to effectively enforce the *Competition and Consumer Act 2010* (CCA), the ACCC recommends that any new regime for communications information should provide that call charge records and reverse call charge records be kept for at least two years.

The ACCC believes the proposed mandatory data retention period of up to two years is appropriate for information allowing subscriber checks and searches of the Integrated Public Network Database to be performed.

If the Committee is minded to support the mandatory retention of communications data for a certain period of time, the ACCC recommends that carriers should not be forced to destroy the data after the expiration of the mandatory retention period.

Stored communications (TOR 2.b.)

The ACCC recommends the Committee take into account the benefit of stored communications warrants to investigation of serious civil and criminal contraventions of the law and not support a proposal to confine its availability to investigation of criminal matters only.

Should the Committee be inclined to recommend a common threshold for stored communication and content warrants, the ACCC recommends that the threshold be set with reference to the types of conduct for which the warrant can be sought, as compared to the type of agencies who can apply for such a warrant.

Proposals for telecommunications interception reform

After thirty years of changes to technology and law enforcement, the Committee is being asked to consider what amendments might be appropriate to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and what features of the existing regime should be retained into the future.

The Australian Competition and Consumer Commission (ACCC) is particularly interested in how these issues are addressed in light of its use of the TIA Act to investigate and prosecute breaches of competition and consumer law. Some of the proposals for change to the TIA Act included in the terms of reference for this inquiry, such as in relation to communications information and stored communications, have the potential to diminish the capacity of the ACCC to investigate serious contraventions of the law.

In this context, the ACCC wishes to alert the Committee to its use, and potential use of:

1. Communications information
2. Stored communications

A key theme in the current law, and one which the ACCC suggests should be retained into the future, is that third parties can only access the content or data associated with a person's communications for lawful purposes. Privacy should remain a key theme in any new regime governing access to communications by law enforcement. That said, the ACCC is strongly of the view that any change to the TIA Act should not reduce its capacity to effectively perform its functions.

ACCC's operating environment

The ACCC is an independent statutory authority which enforces Australia's competition, fair trading and consumer protection laws, contained in the *Competition and Consumer Act 2010* (CCA).

The competition provisions of the CCA apply to every Australian business. Anti-competitive practices that substantially lessen competition, the misuse of market power and cartel conduct are prohibited. Breaches of the law are established through legal proceedings in the Federal Court and may be remedied (and deterred) through injunctions, pecuniary penalties, damages for victims, and for cartel conduct, imprisonment of individuals.

The CCA also contains the Australian Consumer Law (ACL), a set of nationally consistent consumer protection provisions enforced by the ACCC and State and Territory fair trading regulators. Broadly the ACL sets standards of business behaviour by prohibiting firms from engaging in misleading conduct, unconscionable conduct, or making false representations, and protects consumers through its product safety framework.

1. Communications information and data retention (TOR 2.a., 15.c.)

The terms of reference of this inquiry note that the Government wishes to reduce the number of agencies eligible to access communications information (TOR 2.a.). The importance of access to 'communications information', that is information about the process of a communication as distinct from its content, cannot be overstated. Without it, the ACCC would be unable to effectively enforce competition and consumer law.

The ACCC cannot access communications information for investigations for all the prohibitions in the CCA. Further, access is not permitted unless a senior officer has reason to believe that there is a potential breach of the CCA and the disclosure of the information is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty.

Communications information is often crucial to the ACCC's investigation of breaches of competition and consumer law. In cartel cases it can provide the evidence of when calls were made, their origin, destination and duration. This information is often the only irrefutable evidence of contact between cartelists and is critical to successful investigations and prosecutions. In the investigation and prosecution of scam conduct, it provides the name and address of the person behind the telephone, IP number on a webpage or an email address. The ACCC has this capacity now, and has an ongoing need in its investigations to access call charge records, reverse call charge records, request subscriber checks and searches of the Integrated Public Number Database (IPND) to effectively perform its functions of enforcing compliance with the CCA.

Through access to communications information, the ACCC has, for example:

- obtained evidence of the timing and frequency of calls between petrol retailers in connection with price rises, which, when combined with other investigative tools, assisted the ACCC to stop cartel conduct in Victoria.
- confirmed the involvement of individuals in scams, from which enforcement proceedings were taken, the conduct and thus loss to consumers stopped and banning orders put in place to prevent the repetition of the conduct
- been able to break down 'cover stories' put forward by persons under investigation, through demonstrating the inconsistency of the cover story to the objective evidence provided by communications information.

<u>Data retention period (TOR 15.c.)</u>

The terms of reference note that the Government is expressly seeking the views of the Committee on whether communications data should be retained for up to two years (TOR 15.c.). The proposed period of two years mirrors the existing European Union Data Retention Directive.

As noted in the Attorney-General's Department discussion paper to this inquiry, carriers keep data for as long as their business purposes require. This has some positive and negative implications for law enforcement. In some instances communications data has been kept for a number of years, which has helped the ACCC to obtain evidence of long standing anti-competitive practices. On the negative side, which is likely to be the situation encountered more often as carriers have less need to retain the information, is that it will be kept for short periods of time or not at all.

As the business need to retain transactional data diminishes, a mandatory data retention period may be advantageous to law enforcement as it would ensure the availability of data at least for the period of time prescribed by law. The ability to guarantee the availability of communications data some time into the future is particularly important to the ACCC in its investigation of cartel conduct. This is because cartel conduct is secretive in nature and often does not come to light until years after the cartel was originally put into effect by the cartel participants.

In 2011 and 2012, almost two thirds of the ACCC's requests for communications information related to data more than two years old and one third of all requests related to data more than five years old. Interestingly, all of the ACCC's requests for subscriber data and in relation to the IPND were in relation to data up to two years old.

This raises the issue of whether a data retention period of up to two years should be applied across the board. Such a retention period is likely to lessen the effectiveness of call charge and reverse call charge records as an investigative option for the ACCC and particularly so in relation to its investigation of cartels.

The ACCC understands that the Government is looking to implement a tailored data retention scheme based upon need for information and the cost to carriers and Government. A tiered model has been suggested to the Committee whereby smaller providers with fewer customers (and less capacity to store and retain information about communications and customers) have less responsibility, as distinct from no responsibility, to retain data. While the ACCC sees merit in this proposal from the perspective of encouraging new entry into the market, such a regime may encourage the use of small networks for the wrong reasons.

The ACCC recommends that the Committee recognise the benefit of communications information to the law enforcement activities of the ACCC. To ensure the continued capacity of the ACCC to effectively enforce the CCA, the ACCC recommends that any new regime for communications information should provide that call charge records and reverse call charge records be kept for <u>at least</u> two years.

The ACCC believes the proposed mandatory data retention period of up to two years is appropriate for information allowing subscriber checks and searches of the IPND to be performed.

Any new framework should ensure that carriers can keep communications information for as long as their business purposes require. If the Committee is minded to support the mandatory retention of communications data for a certain period of time, the ACCC recommends that carriers should not be forced to destroy the data after the expiration of the mandatory retention period.

2. Stored communications (TOR 2.b.)

The terms of reference note that the Government wishes to standardise the warrant tests and thresholds under the TIA Act. Broadly the TIA Act provides for warrants to be issued to access communications without the knowledge of the parties to the communication in relation to *real time content* (intercepting a telephone call) and *communications stored by a carrier* after they have been sent (email, SMS, MMS, voicemail). At present the legislative thresholds allowing access by warrant to real time content and stored communications vary significantly.

In the main, telephone interception is limited to investigation of serious offences under criminal law where the conduct is punishable by seven years' imprisonment or more. In contrast, stored communications warrants can be issued by a judge for serious contraventions of civil or criminal law involving a fine or pecuniary penalty equivalent to at least $19,800 (individuals) or $99,000 (businesses), as well as for serious criminal offences capable of interception.

The introduction of the concept of a stored communication into the TIA Act (2004) and the need to obtain a warrant to acquire such information from a carrier without notice to the recipient (2006) is relatively recent. Prior to that time the information could be obtained through statutory investigative notices issued by regulators such as the ACCC. The ACCC retains the capacity to obtain stored communications under its compulsory evidence gathering power to a limited extent; where notice is provided to a party to the communication.

The ACCC has obtained stored communications warrants in relation to matters that attract civil pecuniary penalties, criminal fines and imprisonment under the CCA. The nature of the warrant, without notice to the communicants, has allowed the ACCC to gather evidence without risk that the material will be destroyed.

Where the ACCC accesses stored communications via a stored communications warrant, it must comply with the record-keeping, destruction and reporting obligations of the TIA Act. The ACCC's compliance with these obligations is enforced by internal mechanisms and periodic inspections by the Commonwealth Ombudsman.

The discussion paper to this inquiry suggests that implementing a standard threshold for stored communication warrants and content warrants would:

- reduce complexities that relate to the current threshold for access to a content warrant
- provide consistent protection for 'live' and 'stored' content.

Given the disparity between the thresholds for content and stored communications warrants, and the concern noted in the discussion paper that the threshold for content warrants may be too high, the Committee might be asked to consider a middle point between the two thresholds.

The discussion paper suggests one reason for a common threshold for content and stored communications warrants is that technology use and availability has changed. However, at the time the stored communication regime was introduced, a stored communication warrant was capable of capturing a message that was both considered and which the communicant had the opportunity to review, such as email, as well as communications that simply captured the moment, such as SMS, MMS and voicemail. While technology has moved on from that time, the type of communication that can be captured essentially remains the same, as does their value to law enforcement.

The ACCC would be concerned if stored communications warrants only became available for investigation of criminal matters generally, or only for criminal matters subject to imprisonment.

- Such a change would take away a significant benefit of the existing regime, the ability to collect information without risk of destruction and to use it for serious civil or criminal contraventions.
- There would be a significant impact upon the ACCC's investigative capacity if stored communications warrants only became available for investigation of criminal matters punishable by imprisonment for a number of years. While the CCA provides for multimillion dollar penalties for breaches of the law, only one type of conduct, cartel conduct, is punishable by imprisonment (ten years for individuals).

The ACCC recommends the Committee take into account the benefit of stored communications warrants to investigation of serious civil and criminal contraventions of the law and not support a proposal to confine its availability to investigation of criminal matters only.

Should the Committee be inclined to recommend a common threshold for stored communication and content warrants, the ACCC recommends that the threshold be set with reference to the types of conduct for which the warrant can be sought, as compared to the type of agencies who can apply for such a warrant. At present both concepts are relevant to the TIA Act in relation to content warrants, which are only available to interception agencies only. The ACCC suggests it remains appropriate to ensure non-intercept agencies can continue to apply for a stored communication warrant, as necessary.