



# QUEENSLAND COUNCIL FOR CIVIL LIBERTIES

G P O    B o x    2 2 8 1    B r i s b a n e    4 0 0 1

visit us at [www.qccl.org.au](http://www.qccl.org.au)

Committee Secretary  
Senate Legal and Constitutional Committee  
Department of the Senate  
PO Box 6100  
Parliament House  
Canberra ACT 2600  
Australia

Email: [legcon.sen@aph.gov.au](mailto:legcon.sen@aph.gov.au)

Dear Madam./ Sir

## **TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT BILL 2007**

The following are submissions by the Queensland Council for Civil Liberties in respect to the above Bill. These submissions have been substantially prepared by Samir Patel, a university student at Bond University and a member of the Council.

### **CHAPTER 4 – ACCESS TO TELECOMMUNICATIONS DATA**

#### **Part 4-1 – Permitted access to telecommunications data**

##### *General Comments*

In our view legislation should recognise that a government official should only have power to access personal information where that person is possibly exposed to some sanction be it criminal or otherwise pursuant to a warrant issued by judicial officer.

We accept that circumstances may arise which make it impractical to obtain a warrant before access is obtained. Impracticality should be assessed in the context of current technology. If an official exercises a power to access information in circumstances of impracticality, that official must then, as soon as reasonably possible, justify that action to a judicial officer.

In our view this legislation should reflect those principles.

##### *Division 2 – No disclosure of the content or substance of a communication*

“New section 172 makes clear that Division 3 and 4 of the Act cannot be used to access the content or substance of a communication.”<sup>1</sup> The Council supports the provision.

<sup>1</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 2.

### *Division 3 – The Organisation*

“New subsection 175(3) provides that an eligible person must not authorise the disclosure of telecommunications data unless he or she is satisfied that the disclosure would be in connection with the performance by the Australian Security Intelligence Organisation (ASIO) of its functions.”<sup>2</sup>

This provision appears problematic in the sense that it fails to clearly specify the criteria necessary for an eligible member to reasonably believe that the disclosure being sought after would be relevant for the ASIO to carry out its functions. Without providing an adequate justification for the release of such disclosure, the Council is of the concern that such a provision will only serve to further the power given to enforcement agencies and encourage them to read and interpret the provision in its broadest capacity to the detriment of those individuals whose rights are likely to be infringed upon.

With respect to new subsection 176(3), which permits the authorisation to cover access to both historical and prospective telecommunications data,<sup>3</sup> the Council remains concerned with the idea that the provision infringes upon the privacy of those affected for matters on which there may be no appropriate grounds to do so. According to the proposed amendments, prospective telecommunications data (data that is collected as it is created and forwarded to the agency in near real time) is only available to ASIO or a criminal law enforcement agency because of the higher privacy implications of this type of access. While the Council appreciates the high level of security surrounding the disclosure of such data, it cannot overlook the notion that such gestures taken by ASIO or a criminal law enforcement agency may help to do nothing more than facilitate a notion of guilt upon the individual in question, rather than upholding the presumption of innocence an individual is guaranteed under the law in the first place.

### *Division 4 – Enforcement Agencies*

We are concerned like the Senate Legal and Constitution Legislation Committee<sup>4</sup> that there is a present lack of clarity about whether or not agencies can access the contents or substance of the communication without a warrant. We call upon the Government to take the steps recommended by that Committee to ensure that this does not occur. We join Electronic Frontiers Australia in expressing concern as to whether mobile telephone locational information may be allowed to be disclosed by merely a written request under the Chapter 4. As pointed out by Electronic Frontiers Australia in their submission on the exposure draft this might in effect enable tracking and surveillance of individuals' whereabouts for a period of 45 or 90 days without a warrant being obtained. The legislation should not pass until this is clarified.

<sup>2</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 9.

<sup>3</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 10.

<sup>4</sup> Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006

Also, like the EFA, we would oppose new power authorising access to prospective information or documents.

*Division 6 – Secondary disclosure/use offence*

Of specific concern to the Council is the new subsection 182(2) which permits “an enforcement agency to pass telecommunications data on to a third party for specified purposes set out in this section.”<sup>5</sup>

The example provided in the Explanatory Memorandum was “if during the course of an investigation in relation to taxation fraud, the Australian Taxation Office obtains telecommunications data that concerns drug trafficking, the Australian Taxation Office could lawfully disclose this information to a relevant police agency to investigate further.”<sup>6</sup> Section 182(2) of the *Telecommunications (Interception and Access) Amendment Bill*<sup>7</sup> reads as follows:

182 (2) Paragraph (1)(b) does not apply to a disclosure of information or a document if the disclosure is reasonably necessary:

- (a) for the performance by the Organisation of its functions; or
- (b) for the enforcement of the criminal law; or
- (c) for the enforcement of a law imposing a pecuniary penalty; or
- (d) for the protection of the public revenue.

We believe the provision cannot be allowed to be read in the broadest sense. An individual of which disclosure is being sought for should not have to be subject to an investigation that deviates from the primary purpose from which it was initially intended for.

The enforcement agency must go through the appropriate avenues to acquire the necessary warrants and authorisations to follow through on the matter in question.

Just as one would expect police officers to comply with section 156 of the *Police Powers & Responsibilities Act*<sup>8</sup> to ensure that nothing other than what is stated in the search warrant can be confiscated, so too should there be a requirement that when dealing with telecommunications data, enforcement agencies limit themselves as well to only what their initial purpose of what the interception was intended for in the first place.

**CHAPTER 5 – CO-OPERATION WITH INTERCEPTION AGENCIES**

The Council now directs its attention to Chapter 5 of the Interception Bill, which sets out the obligations for carriage service providers to ensure that communications carried over their telecommunications system are capable of being intercepted.

<sup>5</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 13.

<sup>6</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 13.

<sup>7</sup> 2007 (Cth).

<sup>8</sup> 2000 (Cth).

### **Part 5-1 - Definitions**

The definition of interception capability continues to mean “the ability to intercept and deliver content of any of a wide variety of telecommunications services, including voice conversations, emails, instant messaging and web browsing.”<sup>9</sup>

The Council refuses to accept that such powers should be permitted to extend this far to encompass virtually all forms of communication. The proposed means are without question too intrusive on individuals’ privacy rights, and only serve to provide an alternative means for the police and other enforcement agencies to conduct warrantless, and in some cases, completely unnecessary, invasions.

### **Part 5-2 – Delivery Points**

New section 188 brings reference to the manner in which delivery points are to be setup by the carrier or carriage service provider, as approved by the enforcement agency.<sup>10</sup> The Bill defines a delivery point as a predetermined location from which intercepted information can be delivered.

Upon its review, the Council recognizes that in the event a dispute arises between the carrier or carriage service provider and the agency, it is the carrier or carriage service provider that bears the responsibility to ensure that its delivery point is setup at a location that is to the satisfaction of the agency and the Communication Access Co-ordinator. Furthermore, if a location can still not be agreed to, the matter is referred to the Australian Communications and Media Authority (ACMA) which must determine the final location having regard to:

- (a) the configuration of the service
- (b) the relative costs to the carrier and to the interception agency of any particular delivery point
- (c) the reasonable needs of the interception agency
- (d) the reasonable commercial requirements of the carrier
- (e) the location of any delivery points already existing in relation to any particular interception agency

While the Council applauds the efforts made toward ensuring that the ACMA, in having disputes referred to them, give weight to all factors that need to be taken into consideration when establishing where the appropriate delivery point should be, it also recognises that section 188(8) of the Bill directs the carrier to nominate another place if the delivery point suggested by the ACMA no longer remains suitable as a result of a material change in the circumstances of the carrier.<sup>11</sup> Additionally, it also imposes a further responsibility on them to inform the Communications Access Co-ordinator

<sup>9</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 16.

<sup>10</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 16.

<sup>11</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 18.

accordingly as well.<sup>12</sup> The ultimate effect of this provision then is that it places a greater burden on the carrier to ensure that all steps are taken to conform and adhere to the requirements of the agency, regardless of the substantial costs and inconveniences it may sustain as a result.

Instead, the Council proposes that the carriers be allowed to have a greater involvement as to whether in their opinion, it is feasible or not to have a delivery point setup at a particular location. Should it be the case that a mutual decision cannot be agreed upon over time, given valid consideration to the carrier's interest (eg. costs, available technological resources, and the foresight of potential disruptions to general public service), it is of the Council's opinion then that such efforts be aborted, and alternative means of acquiring the necessary information be employed instead. It is also suggested that such decisions will obviously have to be determined on a case-by-case basis by an independent mediator, having regard to how pertinent and urgent they deem the information sought after to be at that time.

### CONCLUSION

In Mr. Ruddock's Second Reading of the Bill, he argues that the Bill, in transferring key security enforcement provisions from the *Telecommunications Act*<sup>13</sup> to the interception act, consolidates and clarifies these provisions to better protect the privacy of telecommunication users. The Council however, remains convinced that these amendments serve only to further disrupt the privacy of these individuals by extending more power to the police and other enforcement agencies to undertake such intrusive conduct without the necessity to present a warrant for being able to do so.

Mr. Ruddock has also deemed it necessary to stress that the proposal does not represent new powers for security and law enforcement agencies, but that it instead, creates new, more systematic and appropriate controls over the existing framework. In our view, Mr. Ruddock is clearly straying away from the obvious, as it would seem that the proposal if nothing else, is simply just an alternative route for enforcement agencies to further impose upon privacy laws whilst hiding behind the legal veil of this Bill.

It is also worth mentioning that with the existing *Telecommunications Act*,<sup>14</sup> carriers such as Telstra were usually left with the responsibility of processing all disclosure requests through a central unit of experienced staff.<sup>15</sup> As a result, if these requests could not be adequately justified, it was within the carrier's discretion to refuse access until a sufficient warrant was produced. It is of the Council's concern then, that under the proposed amendments such powers would be further removed from the carrier since these new provisions ultimately remove the onus for the police and other enforcement agencies to ensure that the validity for such disclosure requests remain strong ones.<sup>16</sup> Furthermore, in the absence of having to produce any

<sup>12</sup> Explanatory Memorandum Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) 18.

<sup>13</sup> 1997 (Cth).

<sup>14</sup> 1997 (Cth)

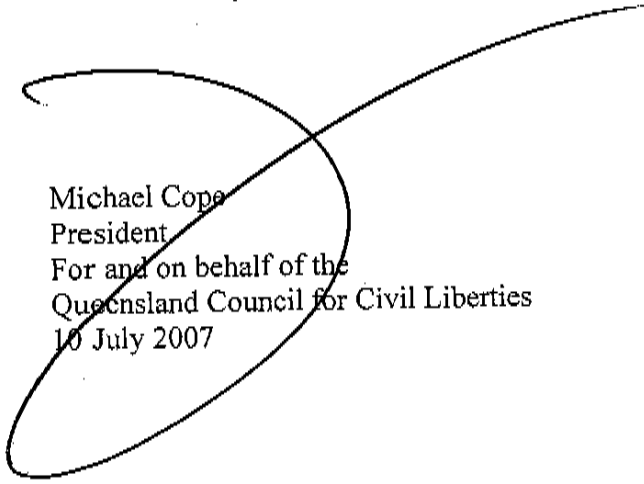
<sup>15</sup> Nigel Waters, 'Telecommunications Interception - extending the reach or maintaining the status quo?' (1997) 4 *Privacy Law & Policy Reporter* 110.

<sup>16</sup> *Ibid.*

kind of search warrant, the proposal simply makes it less difficult for casual routine procedures to be conducted at the sole discretion of the enforcement agencies.<sup>17</sup>

We trust this if of assistance to you in your deliberations.

Yours faithfully



Michael Cope  
President  
For and on behalf of the  
Queensland Council for Civil Liberties  
10 July 2007

---

<sup>17</sup> Nigel Waters, 'Telecommunications Interception - extending the reach or maintaining the status quo?' (1997) 4 *Privacy Law & Policy Reporter* 110.