



COMMONWEALTH OF AUSTRALIA

PARLIAMENTARY DEBATES



**HOUSE OF REPRESENTATIVES**

**BILLS**

**Cybercrime Legislation Amendment Bill 2011**

**Second Reading**

**SPEECH**

**Wednesday, 24 August 2011**

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

---

## SPEECH

**Date** Wednesday, 24 August 2011  
**Page** 9151  
**Questioner**  
**Speaker** Mr ROBERT

**Source** House  
**Proof** No  
**Responder**  
**Question No.**

(Fadden) (NaN.NaN pm)

Mr ROBERT (Fadden) (10:19): I rise to lend some brief comments on the government's Cybercrime Legislation Amendment Bill 2011. Whilst the coalition broadly support the bill, a range of concerns have been raised that coalition speakers have previously moved through. In its simplest form, the bill seeks to require carriers and carriage service providers to preserve the stored communications and telecommunications data for specified persons when requested by certain domestic agencies; to ensure agencies are able to obtain and disclose telecommunications data and stored communications for the purposes of foreign investigations; and to provide for extraterritorial operation of certain offences. It will amend the computer crime offences in the Criminal Code Act and create confidentiality requirements in relation to authorisations to disclose telecommunications data.

The Joint Select Committee on Cybersafety's review of the bill came up with a range of recommendations in their final report. The committee took the approach of ensuring that thresholds that applied to domestic investigation are equally applied to foreign countries seeking access to Australian communications materials. One of the recommendations is that the Australian Federal Police guidelines on police-to-police cooperation in possible death penalty scenarios be tightened and only occur in exceptional circumstances and with the consent of the relevant ministers—in this case, the Attorney-General and the Minister for Justice and Minister for Home Affairs. A range of recommendations like that have been put forward. Whilst we support the objectives of the bill and are broadly satisfied with the safeguards the Attorney-General has put forward, we remain concerned and will watch with great interest to see if the legislation operates as the Attorney-General intends.

There was a range of submissions to the committee, which complained that the convention did not contain sufficiently robust privacy and civil liberty protections to offset the increased surveillance and information-sharing powers it implements. The powers governing the real-time collection and preservation of computer data were identified as being of some concern. However, powers for mass surveillance, such as wire-tapping and eavesdropping—the black arts—are not

enhanced by this legislation because the amendments are limited to telecommunications legislation which still requires the issue of a warrant and does not extend to surveillance devices.

I will make the point that, whilst the coalition broadly support the direction of the bill, we believe that the government must continue to address the issue of cybersecurity not just on a legislative basis but also in terms of our capacity to protect. There is no question that the art of cyberattack is growing and is one of the most pervasive and fastest growing asymmetric means of attack, not only globally but within our region. The Cyber Security Operations Centre, when the then minister—who was two ministers ago; we are now on our third Minister for Defence in four years—launched it in May 2009, was broadly supported, the intent being to maximise the government's ability to detect and rapidly respond to fast-evolving, aggressive cyber attacks. The original funding was something like \$14 million. The intent was to have a continually staffed watch office and an analysis team able to respond immediately to cybersecurity threats as they are detected. The new centre was established in DSD, which incidentally possesses its own significant cybersecurity expertise. It would be good if the government would report back on exactly how the Cyber Security Operations Centre is going, how the 24-hour watch is progressing. It would be good to get some statistics on the amount of asymmetric cyber attack the nation is experiencing.

I am concerned, however, that the former head of the defence department's military cyber unit, Tim Scully, has called on the government to 'speed up its response to the emerging cyber arms race', saying more funding is needed for key civilian agencies. Those comments were reported by Dylan Welch, the *Sydney Morning Herald's* National Security Correspondent. It does bring to the fore the question: is the government doing enough to protect the nation from the threat of cybercrime and to ensure law enforcement agencies and others have access to the legislation they need to be able to do their job?

In terms of the Cybercrime Legislation Amendment Bill, I have taken the Attorney-General at his word that the safeguards are in place and the necessary provisions are indeed there in the legislation for the purposes of law enforcement, among others. But I would stress

to the Attorney-General, who is sitting at the table, that we need to continue to stay at the forefront when it comes to cybersecurity and cyberlegislation to be able to defeat the asymmetric attacks that cybercrime and foreign espionage services will use in this space. It is fundamental that Australia maintains a leading technological edge in dealing with cybercrime and the threat it poses to our national security and our national interests.