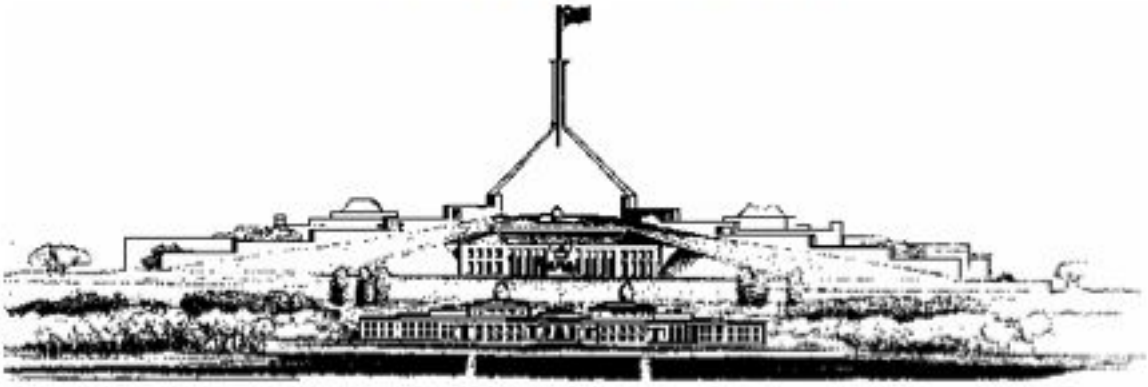
COMMONWEALTH OF AUSTRALIA

PARLIAMENTARY DEBATES



HOUSE OF REPRESENTATIVES

BILLS

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

SPEECH

Wednesday, 18 March 2015

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

SPEECH

Date	Wednesday, 18 March 2015	**Source**	House
Page	2715	**Proof**	No
Questioner		**Responder**	
Speaker	Leigh, Andrew, MP	**Question No.**	

Dr LEIGH (Fraser) (10:16): I rise to speak on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. In considering any bill before the House, it is absolutely vital that we first recognise the status quo. On the issue of telecommunications data, as much as on any issue since the 1999 republican debate, misunderstandings about the status quo have bedevilled the debate about proposals for changing that status quo. So I want to begin by talking about the situation as it currently exists, before the passing of this bill.

At the moment telecommunications companies keep a lot of data about Australians. They keep information about call histories and about the mobile phone towers with which our mobiles have communicated. They keep this information for varying periods of time, sometimes up to seven years.

At the moment this information is accessed a lot. According to the report on the Parliamentary Joint Committee on Intelligence and Security:

In 2012–13, more than 80 Commonwealth, State and Territory enforcement agencies accessed historic telecommunications data under the TIA Act. In total, those agencies made 330 640 authorisations for access to historic telecommunications data, resulting in a total of 546 500 disclosures.

So, at the moment, telecommunications data is being accessed over half a million times a year.

At the moment the range of agencies that are accessing that data is very broad. They currently include: the Department of Foreign Affairs and Trade's passport offices; the Department of Immigration and Border Protection; Racing New South Wales; the Victorian Department of Environment and Primary Industries; the Wyndham City Council; and RSPCA South Australia. So those who argue that we should not pass this bill and should stick with the status quo are effectively advocating for a status quo in which half a million warrantless requests are made annually by agencies that include the RSPCA.

I do not believe this is well-known. Part of the reason for that is the way in which the government has pursued the conversation. On both sides of this, there have been some who have raised extreme concerns. In 2012, one person said of the retention of telecommunications data that it would have 'a chilling effect on free speech'. Another said:

The idea that the government should collect and retain the online records of all Australians for a period of two years I think is disturbing. It appears to go too far and I would have to be persuaded that this was a reasonable request.

On the flip side, one individual said that failing to pass this legislation will cause 'an explosion of unsolved crime'.

We have to put these extremist views to one side. The quotes I have just read into *Hansard* were from, in order, the member for Wentworth, Malcolm Turnbull, in 2012; the member for Curtin, Julie Bishop, in 2012; and Prime Minister Abbott, when speaking this year. You can understand that when senior figures take such extreme views about this legislation that it is difficult to have a reasonable and moderate debate.

It is certainly true that telecommunications data is an important policing tool. Of the half million requests that currently are made, the overwhelming majority are made by policing agencies. The murder of Jill Meagher was ultimately solved using telecommunications data, by matching the cell tower tracking patterns of Jill Meagher's phone and Adrian Bayley's phone. South Australian police have told the Parliamentary Joint Committee on Intelligence and Security that they were unable to re-open a murder investigation because the telecommunications data was no longer available. They said:

A stalled murder investigation was reviewed about 14 months after the victim's death. Fresh information received during the review identified a suspect who was a known drug dealer. The victim, a regular drug user, had been in contact with the suspect and investigators suspect the victim may have been killed over a drug debt. Historical

telecommunications data was sought for the suspect's mobile service for around the time of the murder but it was no longer available.

So the retention of telecommunications data could in that case potentially have helped to solve a murder.

It is into this context—a context of half a million warrantless requests from a range of agencies, including the RSPCA, with few oversights—that the government has moved to change the law.

The bill brought before the House by the c ommunic ations minister last year was inadequate. It lacked appropriate safeguards for the use of telecommunications data. It also lacked an appropriate public conversation about the fact that telecommunications data is primarily used not in counterterrorism operations but in policing operations. That, I think, is one of the reasons why the government has struggled to engage the public on this, because people have felt that this was a new regime. They have felt that, at present, their telecommunications data was not being kept and was not being accessed, and that the government was demanding new rights to store and access telecommunications data.

I believe that it is appropriate to put in place some safeguards around the use of this telecommunications data. Thanks to Labor members on the Parliamentary Joint Committee on Intelligence and Security, this bill has been significantly amended. Those amendments include: listing the dataset in the bill itself, so Australians can know what aspects of our data is being retained; limiting access to telecommunications data to only those enforcement agencies specifically listed in the bill, and not allowing the Attorney-General to add agencies at whim; and providing oversight of the operational use of this legislation by parliament ' s intelligence community—the first time the committee has been given this power, and a step towards beginning to implement the reforms proposed by John Faulkner.

As a result of amendments championed by Labor members, ASIC and the ACCC are able to access telecommunications data to investigate and prosecute white-collar crime. We did not believe that it was reasonable to say that this information could only be available in prosecuting violent crime. We believe that it also should be used to tackle white-collar crime. The report and the subsequent amendments require telecommunications companies to provide customers with access to their own telecommunications data upon request. It requires stored data to be encrypted to protect the security and integrity of personal information. We, on this side of the House, continue to believe that that storage should be in Australia. It does not matter what level of encryption the system has, it is likely to be useless when faced with somebody with physical access to the servers. That means that offshore servers are always going to be less secure in relation to this information than if the information is kept onshore.

As a result of amendments, this bill will prohibit access to telecommunications data for the purposes of civil proceedings, so it cannot be used, for example, in a case of copyright enforcement. On *Q&A* last November it was put to the Attorney-General by Tony Jones that this could be used for prosecutions against internet pirates. The Attorney-General said at the time, 'Well, they can't be and they won't be.' That was not right. As the bill stood at that time, it could be used to prosecute people who illegally downloaded *Game of Thrones*. That is no longer true as a result of the amendments championed by Labor members.

We have required a mandatory data breach notification scheme to ensure telecommunications companies notify customers if the security of their telecommunications data is breached. We have increased the resources of the Commonwealth Ombudsman to strengthen oversight of the mandatory data retention scheme, and we have ensured a mandatory review of the data retention scheme by no later than four years from the commencement of the bill. Importantly, as well, we have ensured that if journalists' data is to be accessed, that must be done through a warrant.

We have ensured that these amendments have been put in place. As a result, I do not want to claim that this is a perfect bill. There are significant challenges in an area such as this where we are balancing the reasonable concerns of law enforcement with the perfectly reasonable concerns of privacy. I would put it to those who argue that this bill is an inappropriate intrusion into personal liberties—and many people have contacted my office with concerns about this bill—that we currently have a system with more than half a million warrantless accesses. We currently have a system where the RSPCA can access your telecommunications data. We currently have a system without oversight from the Commonwealth Ombudsman and without proper oversight from the Inspector-General of Intelligence and Security. So, this system tightens up access to telecommunications data in a way that ought, I think, to give Australians a little more certainty about the access of their telecommunications data.

This is an ongoing challenge for reform. I have little doubt that when parliament comes back to look at this scheme in four years time there will be changes that need to be made. I am also under no illusions that this telecommunications data regime will catch all wrongdoers. But I do believe that it is possible that it might have assisted in the solving of the 14-month-old murder case that South Australian police confronted where telecommunications data had been discarded. It was by chance that the murder victim was using a particular mobile phone whose carrier did not retain the data for as long as other carriers do.

I do believe that this bill puts in place additional safeguards. For the first time, individuals will be able to access the information that is kept about them. For the first time, individuals will have the certainty that the information being kept about them is encrypted. For the first time, there will be appropriate resources given to the Commonwealth Ombudsman in order to oversee the use of these data.

We need to have this debate in an environment of full information. I understand the busyness in so many people's lives as they confront these conversations. The conversation has not been helped by overblown rhetoric such as that, indeed, of Malcolm Turnbull and Julie Bishop in 2012. We do not need to claim that this reform solves all the world's problems, but we do need to acknowledge that the current system is, in some sense, a bit of a Wild West for the agencies that can access it and the oversight that is provided. This bill takes a step along the way towards a better regime for telecommunications storage and access and I commend it to the House.