PAUL FLETCHER

The way to stop firms holding on to our private data

There has been a lot of commentary about the Optus data breach and the sensitive personal information of customers being leaked. The Albanese government, having been slow to respond initially, is now talking about new laws to deal with cyber security. This is rather a curious response because in fact there are tough new laws passed only in the past couple of years by the Morrison government, the Security of Critical Infrastructure laws.

Telecommunications companies are one of 11 sectors covered by the laws. These laws give the home affairs minister extensive powers including to direct an owner or operator of critical infrastructure to take specified actions to mitigate national security risks.

In addition, the telcos face detailed requirements under the Telecommunications Sector Security Reforms, legislated in 2017, to protect networks and facilities from unauthorised access and interference. The secretary of the Department of Home Affairs has extensive powers to require information from telcos on how they are meeting these requirements.

But there is something else the Albanese government should do: move quickly to complete the detailed work program it inherited from the Morrison government to establish a trusted digital identity framework. This would help to solve the basic problem that underlies the Optus data leak and similar leaks that have occurred from other companies and government departments.

The problem arises whenever an organisation collects identity information from me as a customer – name, address, date of birth, driver's licence number, passport number or whatever else it might be – and keeps that information in a database. If criminals succeed in hacking into that database, they can then use my personal information for criminal purposes – for example, by using my personal information to seek to get control of my bank account.

Today, when I go to a bank to set up a new bank account or to a telco to get a new mobile service, I typically provide evidence of my identity through documents such as a driver's licence or utility bill, and that identity information is retained on file.

But imagine if I could establish my identity simply by keying in my name to the website of the bank or telco, then typing in a multi-digit code just sent to me by my "trusted identity provider".

Once I did this, the bank or telco's computer system would electronically be able to access the computer system of my trusted identity provider, which would electronically certify that I was in fact Paul Fletcher and provide one-time verification of other information required – for example, the fact I was over 18.

The advantage of this system is that now my identity data is stored once. I will initially have gone through a process with the trusted identity provider, under which my identity is verified through electronic checks against secure government records such as those of the Australian Passport Office, the Australian Taxation Office, by a state government driver's licence system, and under which I also provide biometric information in the form of a photo of my face taken with my smartphone.

Once my identity is established with the trusted identity provider, I can use it to open a new bank account or customer account with a telco or in all the other situations in modern life where you need to establish your identity. Critically, this would mean the bank, telco or other organisation would not need to store my data. There would be rigorous requirements on the trusted identity provider to maintain the highest standards of security and encryption.

Such a system is pretty much ready to go, following several years of detailed work led by the Digital Transformation Agency under the Morrison government. That included public consultation and, last year, issuing an exposure draft of the Trusted Digital Identity Bill. Already such a system is in operation, through MyGovID, for Australians to deal with federal government agencies. But if the bill becomes law then it will allow other organisations to become trusted identity providers, and it will set out the legal regime for the trusted digital identity to be used to establish identity with private sector organisations and state and territory governments.

Unfortunately, the Albanese government has not shown clear direction on this issue. Government Services Minister Bill Shorten seems more interested in political payback exercises with his Robodebt royal commission than in using digital technology to allow Australians to deal with governments and businesses more efficiently and securely. The Digital Transformation Agency no longer sits with the minister responsible for Services Australia, having instead been transferred into the Department of Finance.

There are lessons to learn from the Optus data breach, and that includes revisiting the customer data retention requirements that apply to the telcos.

But as the Albanese government considers its response, it needs to draw on the extensive work done by the previous government in two important areas. The first is the Security of Critical Infrastructure legislation, which gives the home affairs minister extensive powers.

The second is the trusted digital identity framework, which offers a structural solution to the problem all of us face – every time we hand over our personal information to a company or department, whether that information remains secure is beyond our control and is in the hands of that company or department.

Paul Fletcher is opposition government services and the digital economy spokesman. He is a former Optus executive and the former communications minister.