How plausible is the claim, by independent MP Craig Thomson, that union rivals may have “cloned” his phone? On Monday, he told Parliament his phone could have been cloned as part of an elaborate conspiracy to implicate him in the use of prostitutes.

Opinion seems divided as to how easy it is to clone a mobile phone. Some say it’s a straightforward matter, others that it’s the province of super-spies only.

Of course the easiest way to prove that it was straightforward would be to actually do it, but it’s not quite that simple.

Not all mobile phones are the same. The ease with which they can be cloned depends on a number of things: access to the phone, the type of network and the type of phone. It also depends on what is meant by “cloning”.

If we mean building an exact replica of the phone, that’s clearly a substantial challenge. But if it just means constructing a phone so that embarrassing calls made on the cloned phone appear on the bill of the other phone, that’s a quite different matter.

Let’s use the second definition.

When the calls in question were made in 2005, there were two main cellular network technologies operating in Australia - CDMA and GSM. The CDMA system was used mainly in rural areas and was shut down in 2008, whereas GSM was and still is, in use across the country.

By all accounts, cloning a CDMA handset is not difficult. It does, however, require a couple of things:

- access to the phone in question
- that either the PIN of the phone is known or is not set.

Assuming the person or persons carrying out the cloning had access to the phone then the next step is to obtain the phone’s Electronic Serial Number (ESN). In CDMA networks the ESN is used to link the phone to a particular account.

For popular models of handsets, the ESN is surprisingly easy to obtain from the phone itself. If the phone is not protected by a PIN, obtaining the ESN can be obtained with only a few keystrokes.

After obtaining the ESN, the next step is to purchase another phone and modify its ESN to be that of the original phone. Calls now made from the second phone will have the same ESN as the first phone and will appear on the bill of the first phone. So, if Mr Thomson’s handset was a CDMA one then his story is quite plausible.

If his phone was a GSM handset the story is much more complicated. How old the handset becomes an important issue. Unlike CDMA systems, GSM phones use a Subscriber Identity Module (SIM) card to link a handset to an account.

Cloning a handset in the sense we’re using the term boils down to cloning the SIM card – and that’s not straightforward. The SIM card is protected by a secret key. But there are some weaknesses in one of the algorithms used in the handset known as COMP128.

There are two versions of COMP128. Version 1 has been compromised. Where the SIM card uses version 1, it is possible to purchase devices that clone the SIM card.
Whether they were available back in 2005 (the period in question in the Craig Thomson story) is a question I don’t have an answer to. But, provided the SIM card was using version 1 of COMP128, it is possible that a copy of the SIM card could be made and then placed in another phone and calls from that phone appeared on the bill for the other phone.

But there are other issues. Some phone companies do not allow SIM cards to be swapped from one phone to another. Each GSM handset has several identifiers apart from the phone number.

There is an identifier associated with the SIM card (the International Mobile Subscriber Identity or IMSI) which links the handset to the account, and an identifier associated with the handset itself (the International Mobile Equipment Identity or IMEI).

The IMEI is burnt into the handset at the time of manufacture. Both these identifiers are transmitted to the network when a call is made. Carriers that prevent SIM card swapping keep a record of the IMSI and its associated IMEI.

If the IMEI is different to what’s recorded, the SIM card has been swapped to another handset and the network will reject connection attempts. So we have yet another question: did Mr Thomson’s carrier prevent SIM card swapping?

Even if it did, that’s still not the end of the story. The carrier prevents SIM swapping by linking IMSI and IMEI. If the IMEI can be changed then the restriction on SIM card swapping could be avoided …

I think that’s probably a good place to stop. Maybe falsifying an IMEI is not super-spy territory, but we are getting there.

Whether or not it would be easy to clone Mr Thomson’s phone depends on many factors. Whether it was CDMA or GSM, whether or not it was a well-known brand; if it was GSM, how old it was; whether the carrier prevented SIM swapping; how much access the person or persons allegedly doing the cloning had to the phone – and so it continues.

In a nutshell, unless more information is forthcoming, it’s difficult to assess how plausible Mr Thomson’s claims are.