SAFEWA APP — ACCESS — POLICE INVESTIGATION

224. Ms M.J. DAVIES to the Premier:

I refer to revelations yesterday that the Western Australia Police Force accessed SafeWA app private data.

(1) Can the Premier confirm that WA Police have made at least seven attempts to access SafeWA data, not two, as he indicated yesterday?

(2) How many SafeWA user details have been accessed by WA Police?

(3) Can the Premier provide an ironclad guarantee that there has been no commercial sale of private information captured by the SafeWA app?

Mr M. McGOWAN replied:

I thank the member for the question. Before answering, can I also acknowledge the students from the Shenton College Deaf Education Centre who are here this afternoon. Thank you all for your attendance. I understand you have been in the library with the famous Fiona, unveiling a painting. It is great to have you all here, students.

On behalf of the member for Pilbara, I also acknowledge members of the Western Desert Lands Aboriginal Corporation—in particular, the chair, Melvin Farmer; deputy chair, Anne Mitchell; and directors Colin Peterson, Lindsay Robinson and Darryl Jones, who have come down from the Pilbara. Thank you for joining us, together with CEO and former member of Parliament Tony McRae. It is great that you are all here.

(1)–(3) I thank the member for the question. I largely answered this question yesterday, and I answered it today at a press conference. What occurred was this. I will go through each of the member's exact questions. We put in place the SafeWA app last year in response to the COVID outbreak so we could have a rapid measure to contact trace people who might have been at premises where a positive case had been. The system itself is actually quite brilliant and there have been 245 million uses of it since we put it in place. We made it mandatory on 5 December last year.

The view was—certainly, my understanding was—that it was not to be used for any purposes other than contact tracing. As the member knows, because we have all used it, the information is encrypted. You use your phone to click on the QR code and that information is encrypted and collected by Health, only for the use of contact tracing, as was our understanding of it.

We found out in April this year that on a couple of occasions the police had accessed it, once to investigate a very infamous murder. My understanding is that they accessed it in order to work out who might have been a witness—who was at the event who might have clicked in quite innocently, but might have seen or observed something in the commissioning of this murder that might have been relevant in terms of evidence. I can understand why the police did that; I think we can all understand why a detective might have thought that that was a piece of information that he or she might have wanted to acquire.

When I learnt of this, the ministers and I discussed with my staff what we could do about it. I met with the Commissioner of Police on a couple of occasions and certainly discussed it on a few occasions with him. His view was that it was lawful under the existing law for detectives to access this information and that for him to tell them, particularly in these sorts of extreme cases, that they could not access lawfully available information would not be right. That was his view. I said that I understood that point of view and that it was a very legitimate point of view, but that we needed to make sure we did not discourage people from using the contact tracing app in any way, shape or form, so therefore we would prefer that the police did not use it. He was not able to give us that assurance.

To the best of our knowledge—I am advised by police—it was used on two occasions in relation to two serious crimes, where they tried to obtain information largely around who might have been a witness. These are two separate occasions out of 245 million uses of the app.

In relation to those two cases they were, as described to me, exceptional cases. One was an infamous murder and the other was a serious grievous bodily harm. Obviously, our legislation will prohibit that from occurring again. The information is encrypted. We have done everything we can and, as far as I am absolutely aware, there is no use of this information in any commercial way, except to say that when you fill out a register in a cafe—we have all done it, and I assume the member has done it—someone like the cafe owner might go and look at it, or whatever. The legislation is designed to ensure also that that information is destroyed after 28 days.

That is what has occurred. We obviously would have preferred this not to have occurred, but it is very explainable. We have been completely above board and we intend to make sure that this situation is repaired.