176. Dr Marczak first publicly linked a case of spyware installation attributable to NSO by examining the behaviour of a device on clicking on a link in a malicious text message which had been sent to Ahmed Mansour, a human rights activist from the UAE. As a result of that examination, Dr Marczak was able to establish that the information received by the device when that malicious link was clicked on had certain 'fingerprints' which were also evident in responses communicated from a series of other IP addresses. Some of those IP addresses pointed to domain names registered to NSO. Dr Marzcak concluded that the set of servers linked to those IP addresses was associated with Pegasus: Marczak 1, [9]-[19].

177. By a means of a technique called DNS Cache Probing, Dr Marczak was able to search for other devices which had repeatedly looked up Pegasus C&C Servers and which had therefore probably been infected with the Pegasus spyware. This enabled Dr Marczak to identify that a device which belonged to Mr Abdulaziz had been infected in this way: Marczak 1, [20]-[24].

178. Dr Marczak then divided up the servers associated with Pegasus into 36 groups (which he terms 'operators'), with each group/operator representing proxy servers which communicated with a single Pegasus C&C server. By examining the traits of each group of servers/operator, Dr Marczak was able to identify that some of them were linked to a particular country. This identification was made by reference to: (a) the domain names relating to a particular operator; (b) the identities of targets who had received malicious text messages containing links to domain names relating to a particular operator; (c) country themes suggested by those domain names (eg where they impersonated websites relating to a particular country); and (d) DNS cache probing results showing the countries on which the operator was probably spying. See Marczak 1, [25]-[26].

179. Dr Marczak identified one operator which he concluded with high confidence was linked to Saudi Arabia, namely KINGDOM). He explains that the basis for this conclusion was that (a) this was the only operator whose domain names showed likely infections in Saudi Arabia based on Dr Marczak's DNS Cache Probing results; (b) Kingdom servers were associated with malicious text messages identified (at that stage) as having been sent to three targets associated with Saudi Arabia: Mr Assiri, Mr Abdulaziz and the Amnesty International researcher working on Saudi Arabia issues; and (c) the domain names employed by Kingdom included names thematically indicative of an Arab kingdom: Marczak 1, [27].

180. Furthermore, Dr Marczak is not aware of any additional targets of KINGDOM that are not clearly linked to Saudi Arabia, and he is also unaware of any individuals clearly linked to Saudi Arabia who were targeted in 2017 or 2018 by a Pegasus operator other than KINGDOM: Marczak 2, [11].

181. On 6 November 2018 Dr Marczak was contacted by Thomas Fox Brewster, a journalist at Forbes magazine, who alerted him to the Claimant's case. The following day Mr Brewster sent Dr Marczak a photograph of a text message on the Claimant's device containing a link to a website (sunday-deals.com) which was one of those Mr Marczak had previously identified as associated with KINGDOM: Marczak 1, [28]-[29].

182. On 16 December 2018 (after Mr Brewster had published an article about the Claimant's case in Forbes), Dr Marczak examined two of the Claimant's iPhones. He identified several