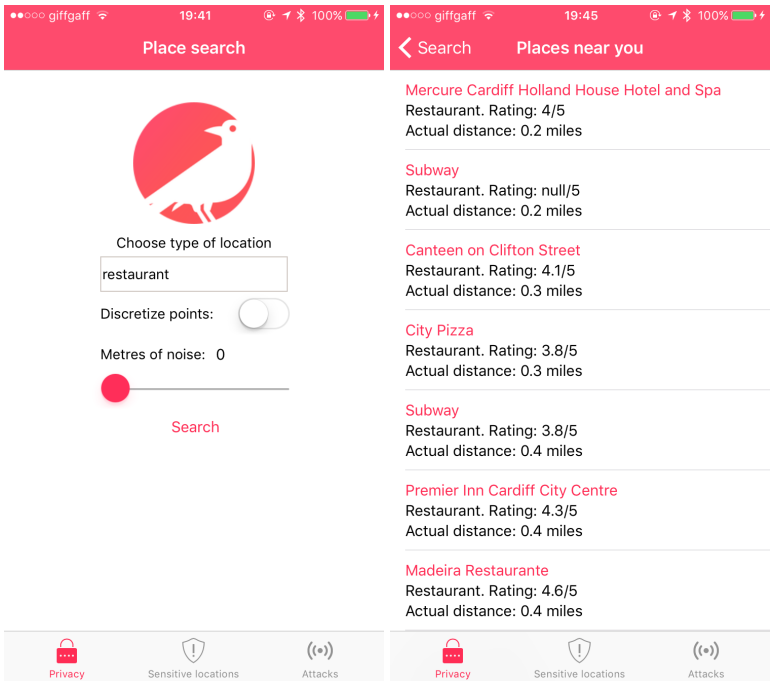
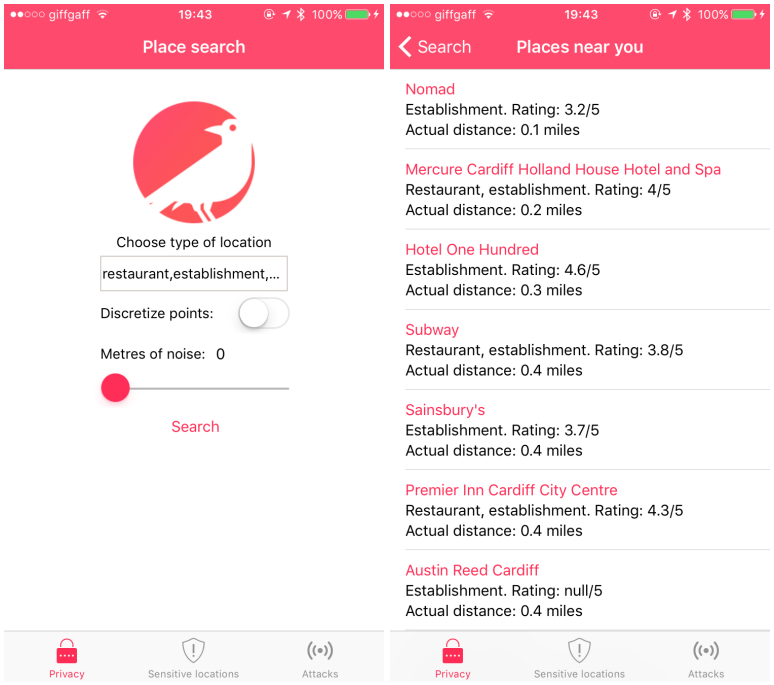
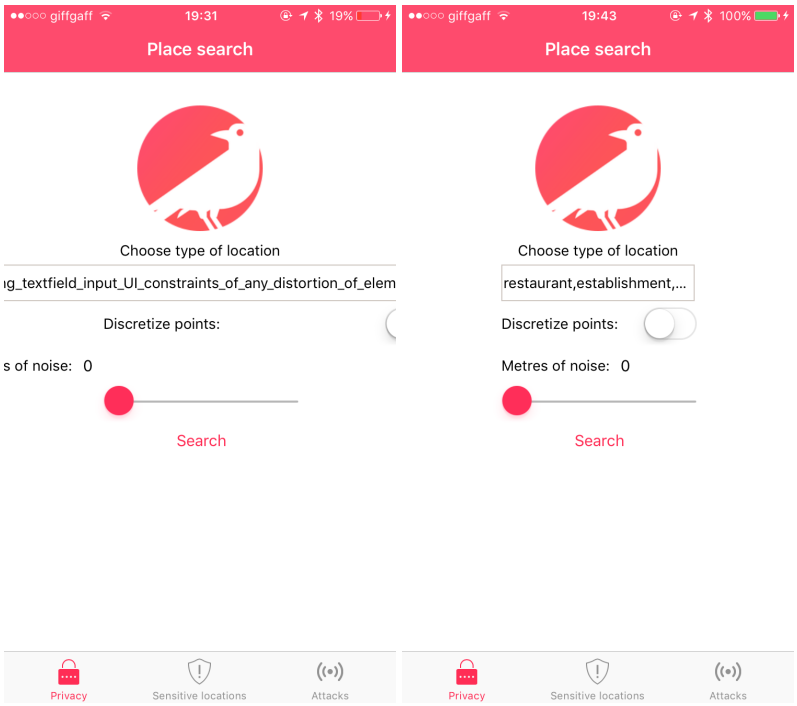
Appendix A



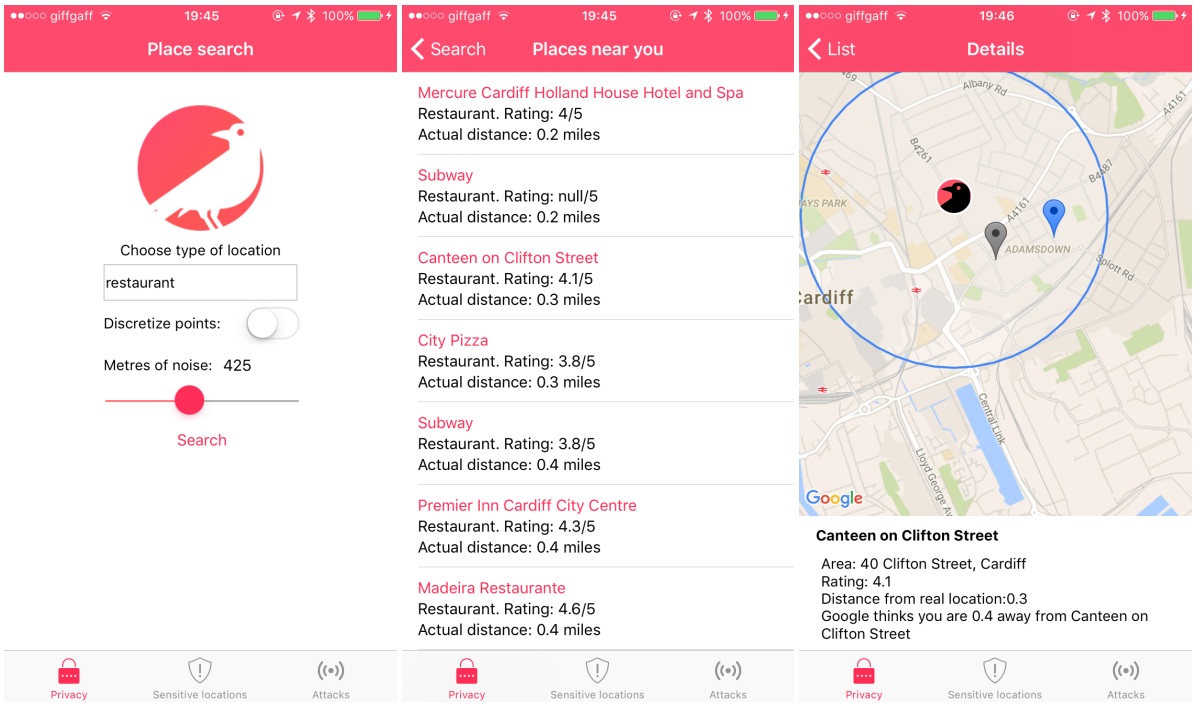
Test 1: Entering a single place type successfully results in a valid response.



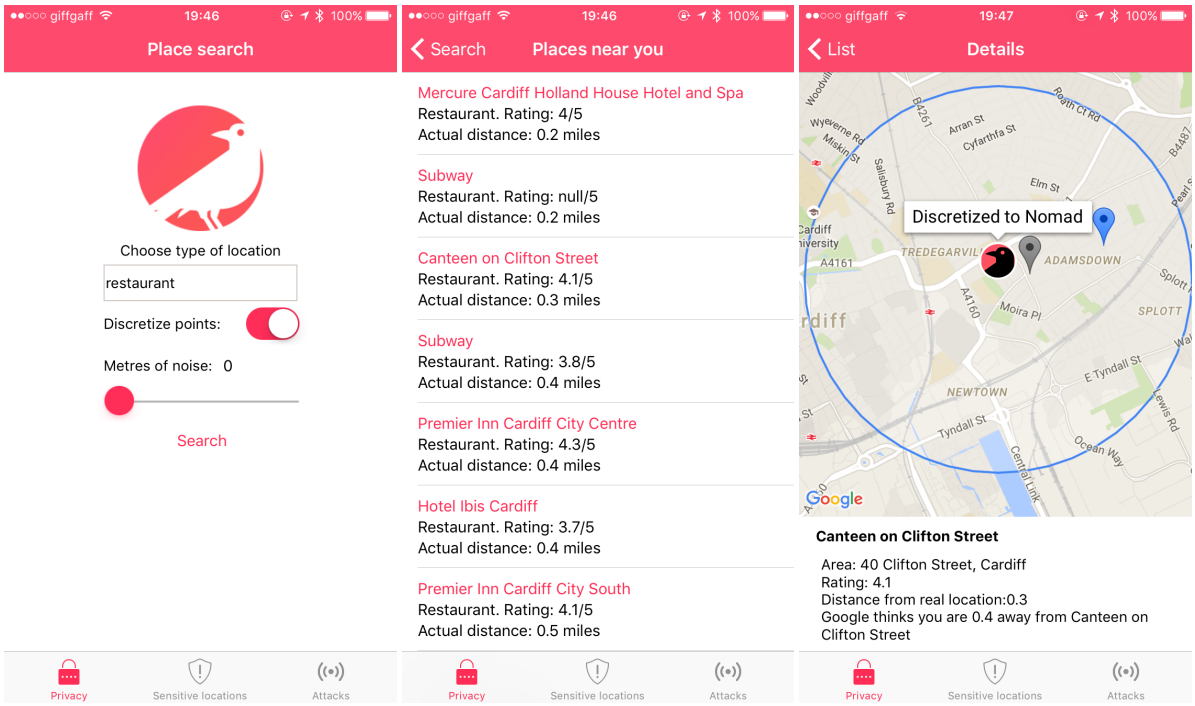
Test 2: Entering multiple place type successfully results in a valid response. Google's API does not always return results for multiple place types, this is an issue with the API, tested also through a browser request (see Appendix-B).



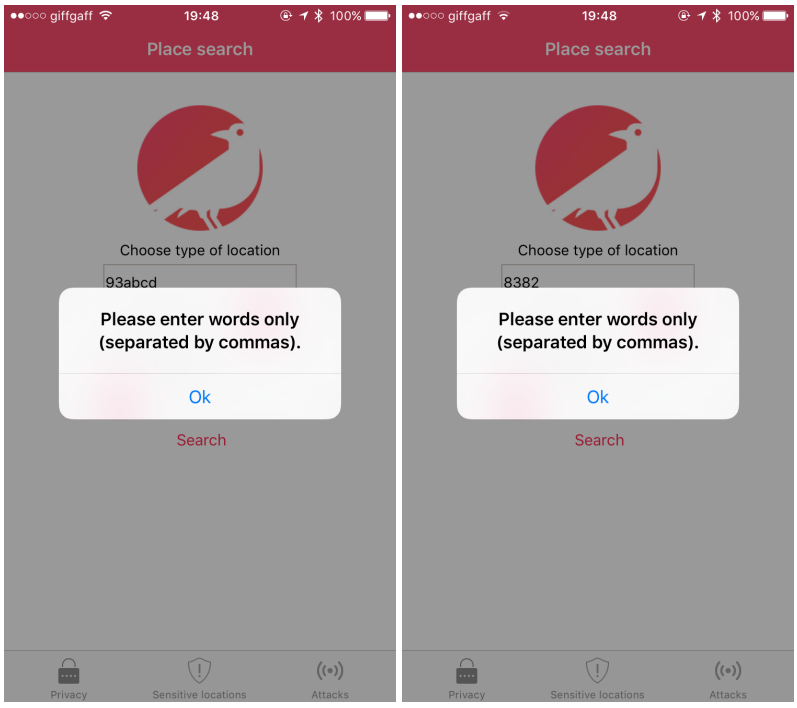
Test 3: The textfield stretched and caused distortion (left). This was rectified with UI constraints to ensure no stretching took place (right).



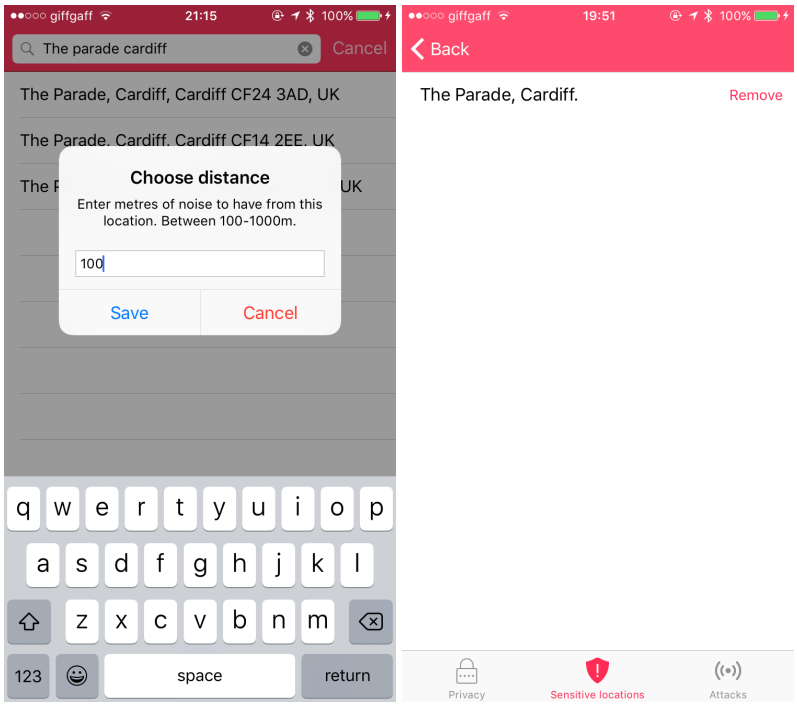
Test 4: Only additive gaussian noise is added, resulting in a successful retrieval of data.



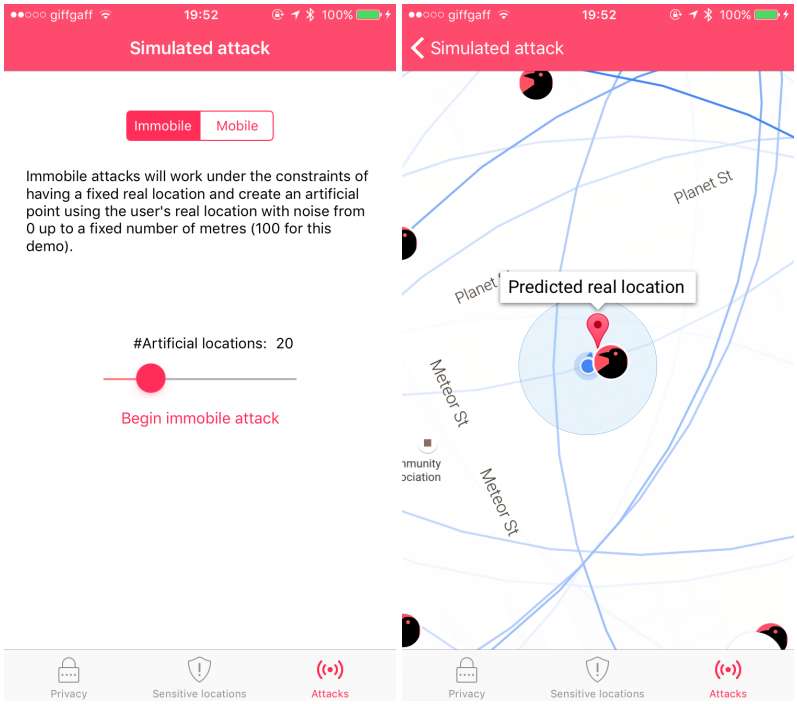
Test 5: Only discretize points is selected, resulting in a successful retrieval of data.



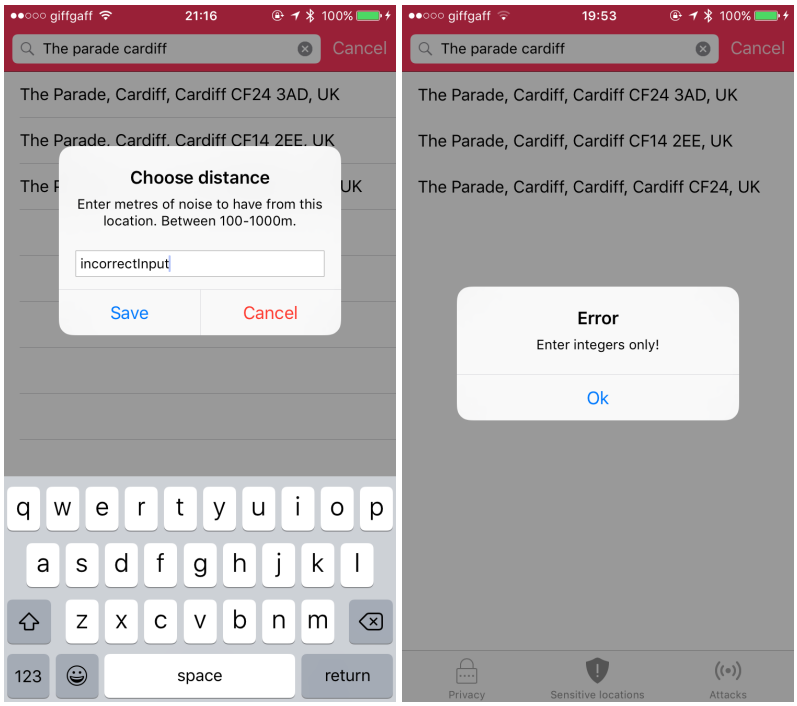
Test 6: A mixture of integers and letters are entered into the text field (left) as well as integers only (right). Validation warnings are presented.



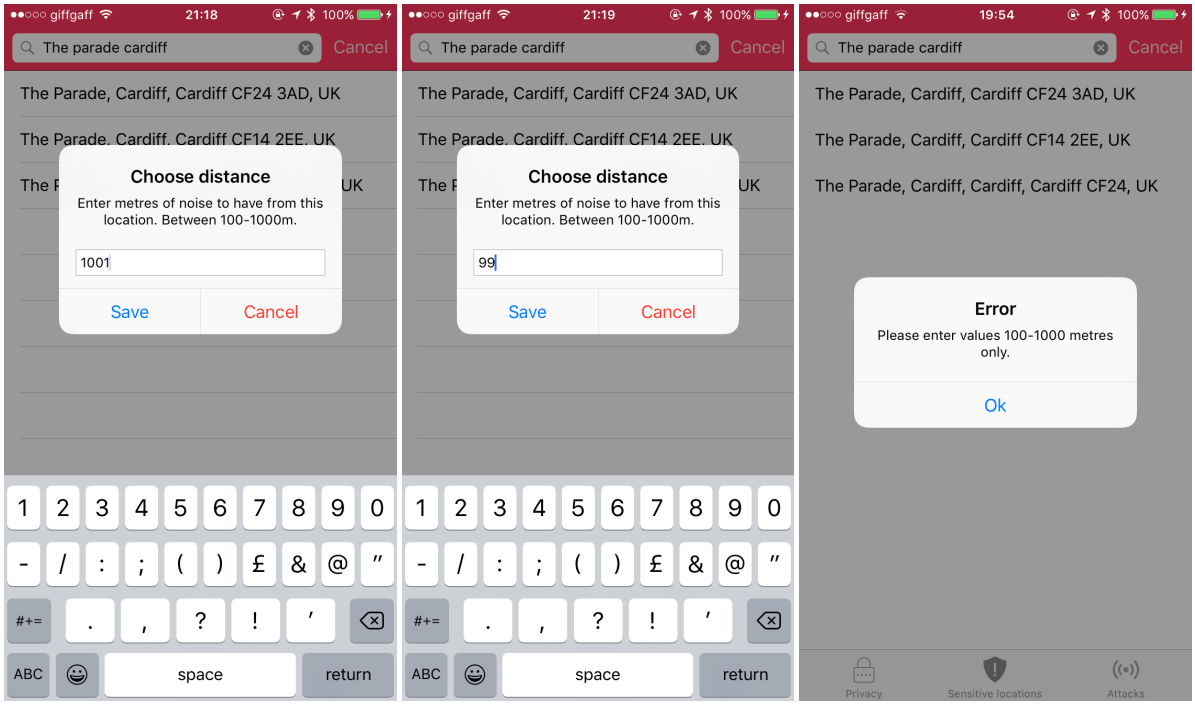
Test 7: A sensitive location is added with the correct input given, in integers, and this is added into the manage sensitive locations panel (right).



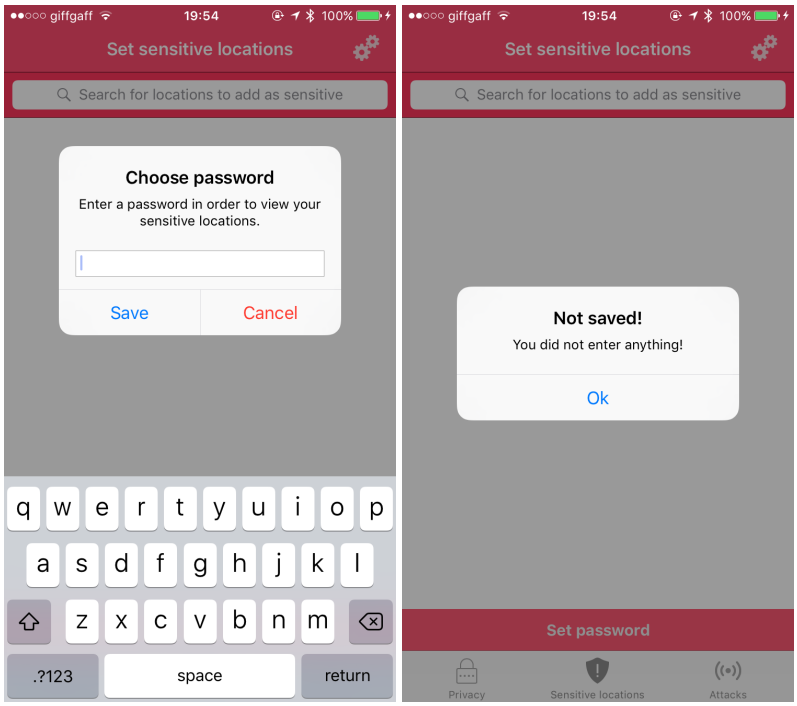
Test 8: An attack is conducted with an arbitrary number of artificial locations generated from a fixed location, which can be used to reverse-engineer a user's real location.



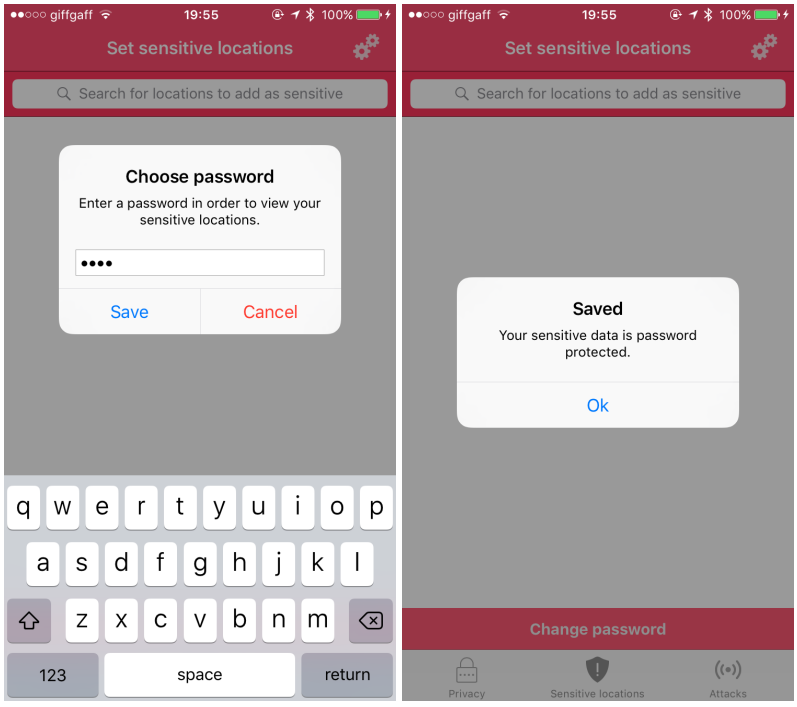
Test 9: String input is entered instead of integers, when specifying, a warning is given to the user specifying to input integers only.



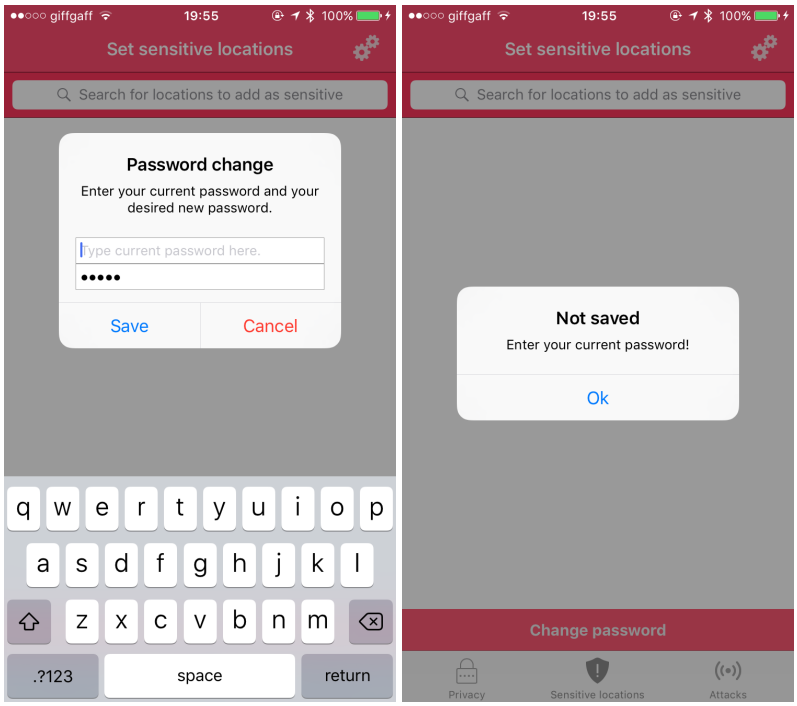
Test 10: When saving a sensitive location, if supplying noise levels outside 100-1000 metres, an error is given to the user.



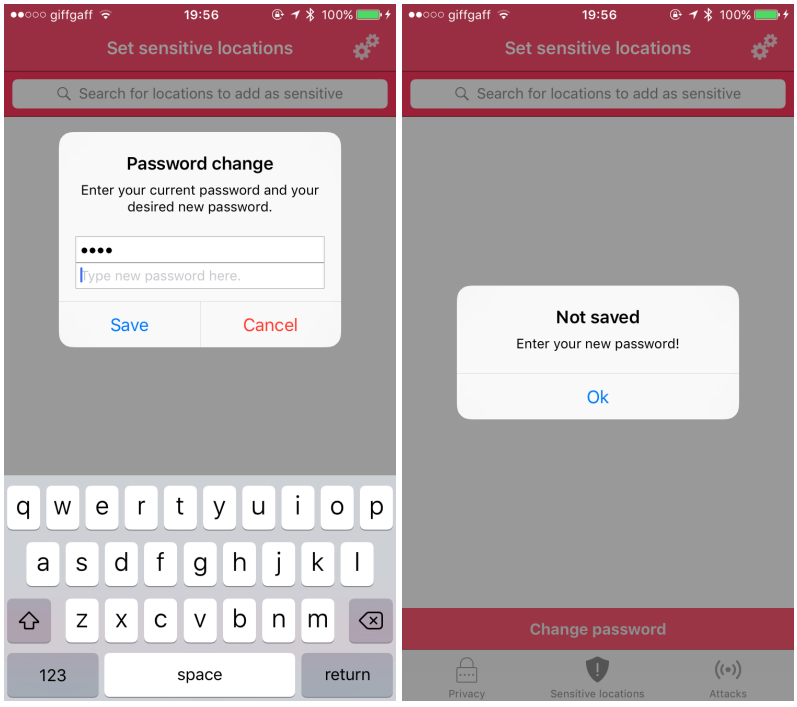
Test 11: When setting a password for the sensitive locations management panel, if a blank password is supplied, a warning is given.



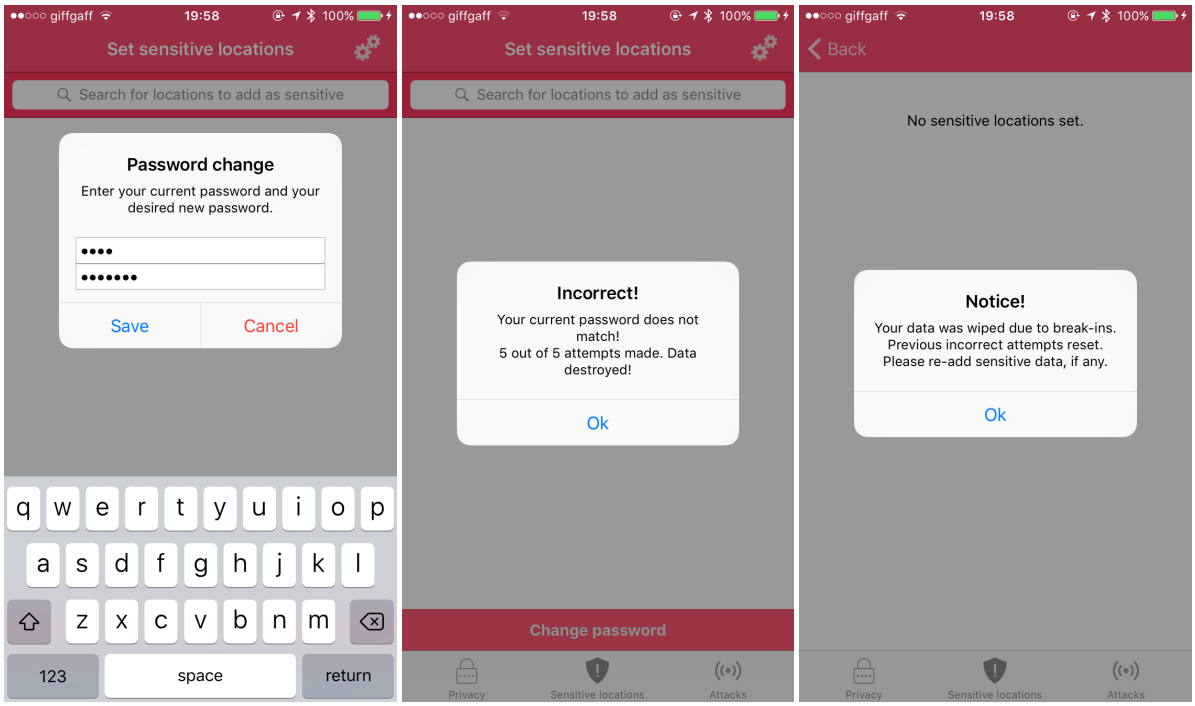
Test 12: If the user supplies input when setting a password, a pop-up notifies them that their sensitive location data will be password protected.



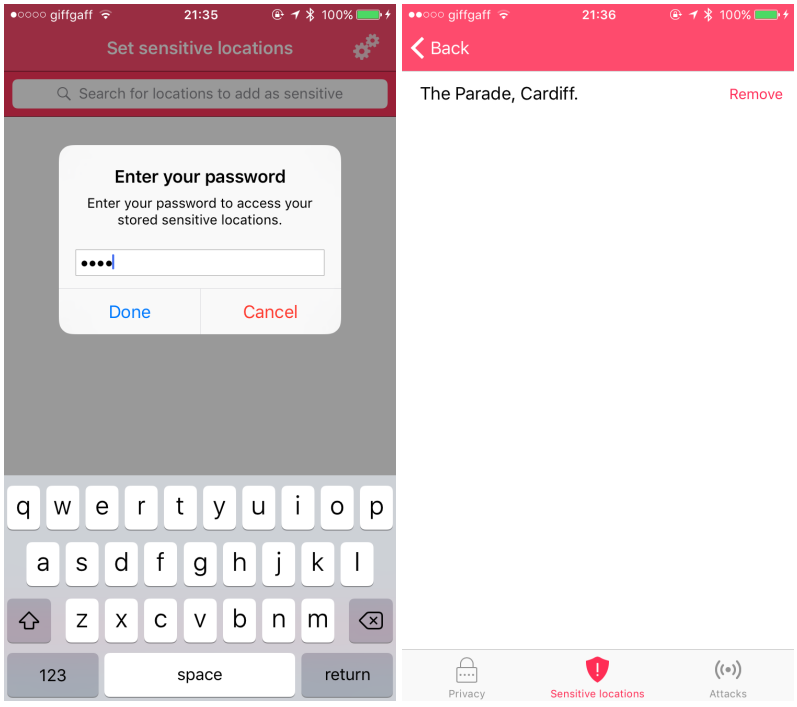
Test 13: When changing the set password, when supplying a new password however no current password, a warning is given to the user to enter their current password.



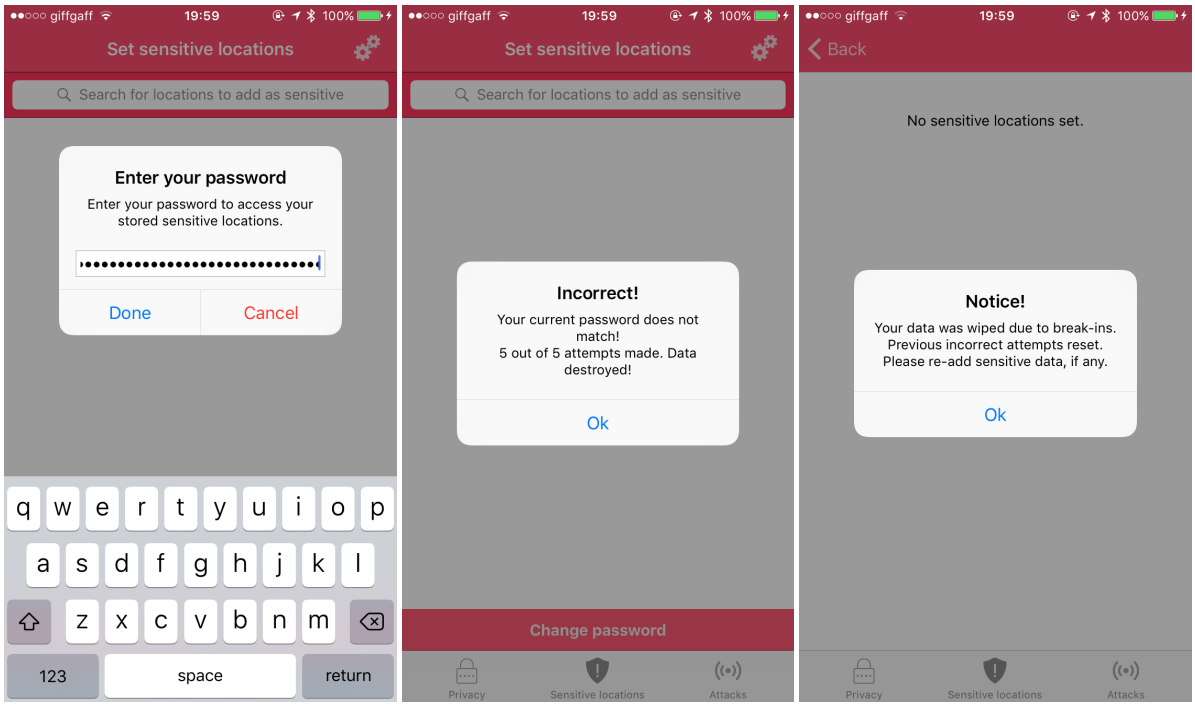
Test 14: When changing the set password, when supplying the current password however no new password, a warning is given to the user to enter their desired new password.



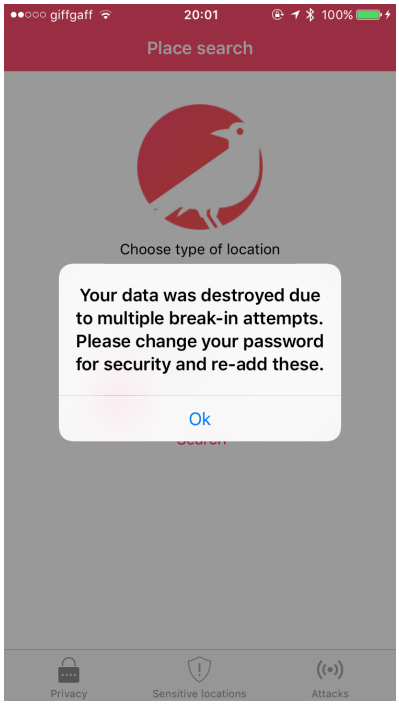
Test 15: When changing the set password, if supplied the incorrect current password, attempts up to five are counted, and when reached, sensitive location data is destroyed.



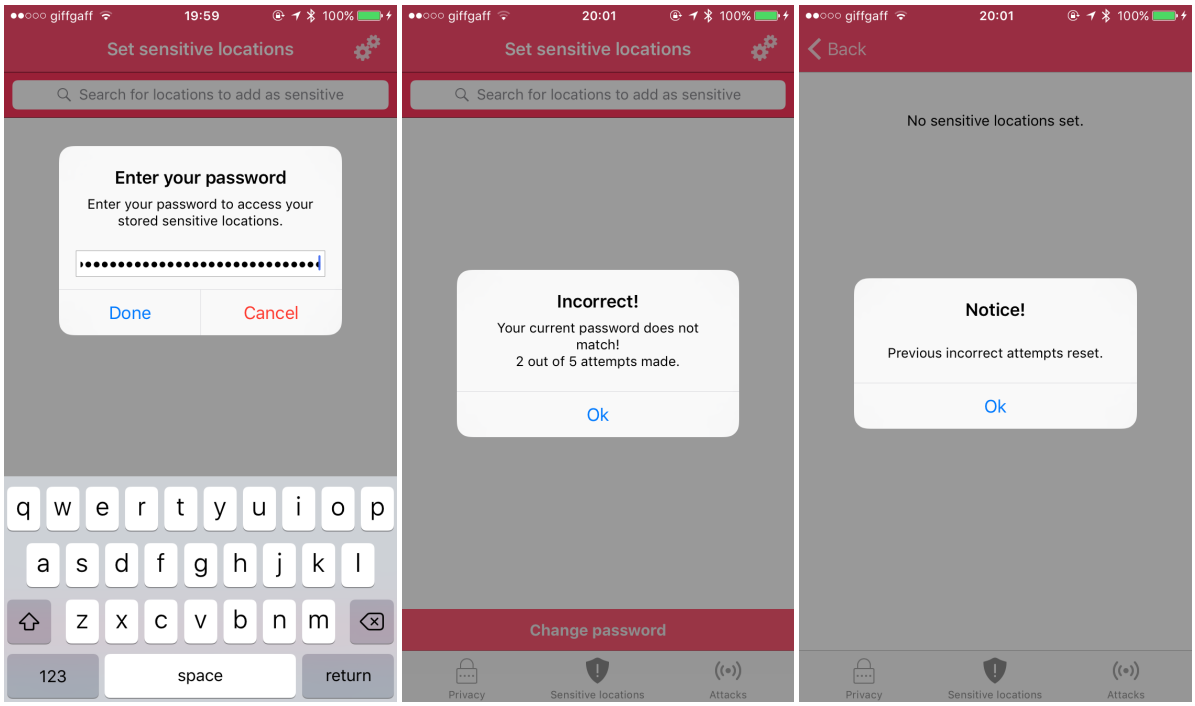
Test 16: If accessing the saved sensitive locations panel, when the correct password is supplied, the user is granted access successfully.



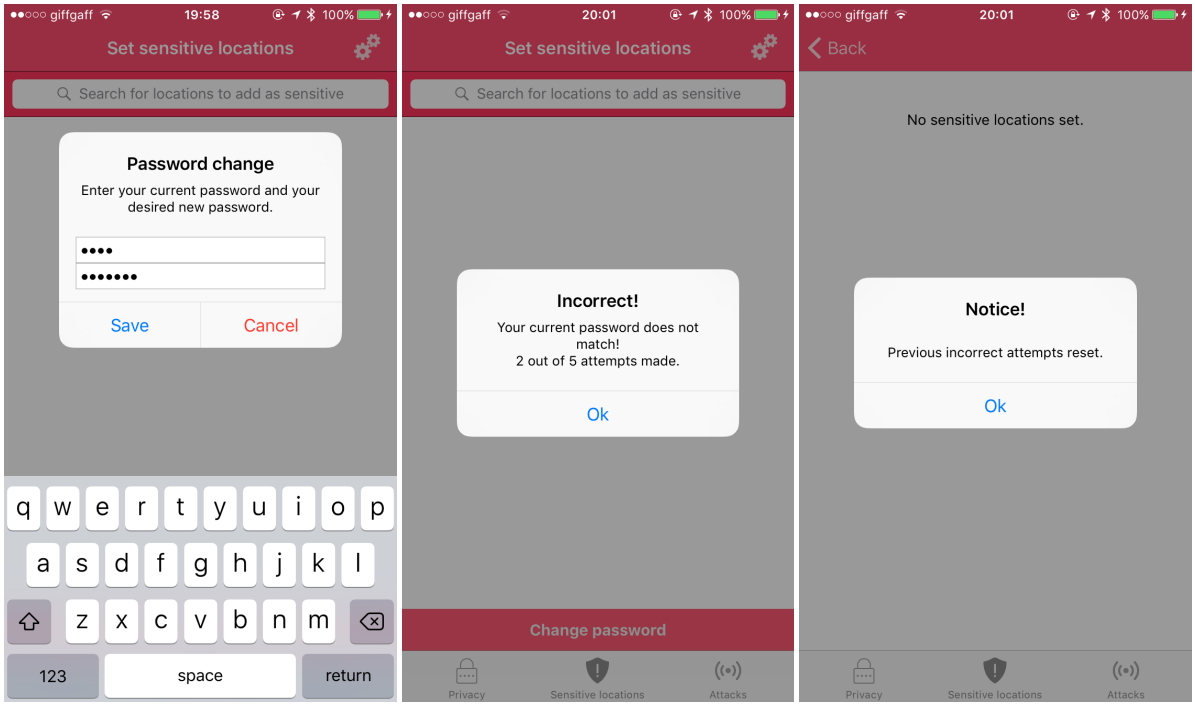
Test 17: If directly attempting to break into the sensitive locations panel by entering incorrect passwords, attempts up to five are counted, and when reached, the sensitive location are destroyed.



Test 18: When data has been destroyed and failure attempts have not been reset through a successful login, each time the user uses the privacy tab, they are alerted that sensitive locations were deleted.



Test 19: If incorrect password is entered to access the manage panel, failure attempts are counted. If access succeeds with the correct password, previous failure attempts are reset, whilst attempts have not reached the maximum limit.



Test 20: If changing password and entering an incorrect current password, failure attempts are counted. If the manage panel is accessed with the correct current password, before the attempts limit is reached, any previous failure attempts are reset.