9.3 Question 3

9.3.A Are there cases, where the identity confidentiality in LTE might be compromised? Explain why. Would that be dangerous?

Terminal Identity Confidentiality
In ESP the UE only sends the IMEI (or IMEISV) if NAS security has been activated. Hence, in this case there would not be any problem.

User Identity Confidentiality
In order to secure the user's IMSI a temporary identity called GUTI is used. So if the network is using the signaling confidentiality property any attacker cannot read the GUTI which is sent from the UE to the MME. However, if signaling confidentiality is not given an attacker might determine a relation between the GUTI and the IMSI. This security problem leads to the leaking of the users place and tracking would be enabled by observing his temporary identities.