# Use Context

- I will maintain my copy at [Consent for Mobile Credentials - MgmtWiki (tcwiki.azurewebsites.net)](https://tcwiki.azurewebsites.net/index.php?title=Consent_for_Mobile_Credentials#Use_Context)

Author Tom Jones 2022-07-28

* It is difficult to make generalizations about what a user needs to see to make a consent decision other than the broad categories of:

1. Who is asking for my data?
2. Why are they asking for my data (what is their specific purpose in asking)?
3. What data do that really need and what is above and beyond what they need?
4. When and where will my retained data be used?
5. Where is the request being made (to the extent that this location contains any information important to my decision)?
6. How will they determine who is requesting access and will that process result in biometric data leakage?

* There are many shown in great detail at this [link](https://kantara.atlassian.net/wiki/spaces/PEMCP/pages/2097325/User+Stories). The paradigmatic edge use cases are:

1. Going through the security line at the airport will typically involve some sovereign entity which is obligated to proof the user before access to the planes.
   1. Who is the airline as agent for the government security checks.
   2. Why the data is needed (purpose) is to prevent hijacking attacks.
   3. What data is needed is dependent to some extent on the holder, who needs to prove that they are not a risk.
   4. When will the data be collected is at least 24 hours before the plane leaves and retention is variable but does trend to complete erasure eventually?
   5. Where the data is collected is likewise variable, but typically begins when the airline crates a flight record(s). The holder should be able to trust the airline collecting that data.
   6. How can the holder know who sees the data? That can be determined, but only by diligent inspection of the rules and regulations, or the holder can trust the governing authority to protect their data.
2. Getting a glass of wine at the locally owned restaurant will typically involve showing the mobile credential to some checker at the restaurant.
   1. Who is the local restaurant, but if the solution is well-constructed, this ID is just to let the user agent know that the verifier is trustworthy?
   2. Why (purpose) is because the holder wants access to a substance that is controlled by a state that sets the rules.
   3. What data is needed is determined by the local liquor board but is being standardized by the ISO 18015 standards processes.
   4. When should be limited to the access point and retention should be limited to meeting state reporting requirements?
   5. Where the data is collected should be clear by proximate location of the liqueur dispenser. Note that is also possible to acquire some sort of token, like a plastic armband to use at the dispenser.
   6. How this happens in being addressed in 18013-7, but potentially by guidance from local standardization efforts like PEMC in North America.