If we want TextSecure to compete with W\*\*\_sapp, F\_book and other less privacy/security focused apps and plattforms, it has to be as user friendly as them. And it should be. Otherwise it'll never get a significant market share with the average users.  
  
But we also want to provide maximum security for people who depend on it with their lives, maybe because they live in an undemocratic country and have an unpopular opinion, maybe because they are protesting the regime in Syria, maybe they are gay and happen to live in Uganda or any of the other 82 coutries where that can get you in jail or even executed.  
  
  
  
As TextSecure is supposed to be secure \*\*and\*\* user friendly there are going to be more and more cases where we will have to decide on a default behaviour, often between the safer and the more convenient option.  
  
Many of the convenient features, which many users want, because they know and love them from W\*\*\_sapp, F\_book and other less privacy/security focused apps and plattforms leak data, which, in some really bad cases, could lead to people getting hurt or worse.  
  
  
  
An example would be a notification popup with the message content like #798 requests. In some cases even mentioning the sender alone can be a threat (#308 and #366).  
  
It gets really bad if this can even happen on a locked phone (#198).  
  
  
  
If we neither want to force the average user to go deep into the advanced settings to manually activate all the features they expect (really bad usability) nor want to endanger some users by choosing insecure but convenient defaults, we should ask the user at the setup level what their use case is:  
  
- casual user  
  
- moderately security concious user  
  
- tinfoilhat™ / protester in $nodemocracyhere   
  
  
  
Based on their choice we'll set default settings for the above mentioned features, as well as security features like #175, #226 and #328 and future convenience features.  
  
  
  
It should also be possible to re-run this from the advanced settings.  
  
  
  
One of the most important presets for the paranoid mode would be to turn off SMS messages entirely, because the metadata, which is the most important tool in modern surveillance, can't be hidden. The network providers can also easily scan the traffic and find out who uses TS, which will put people at risk.  
  
  
  
With data that problem doesn't exist, because the relay (GCM) probably isn't controlled by the "enemy" and it works like an anonymizing proxy, because lots of normal apps use GCM.  
  
As long as HTTPS (TLS) isn't broken (again...), data should be safe.