Public, Secret, Private

- Secret:
  - Secrets are things that are not meant to be shared.
  - Shared secrets are meant to remain within a well defined group,
  - Shared secrets are not meant to be shared outside that group.
- Example: Password
  - Website cannot afford to keep a password; just check the crypto-hash

Public information

- Public information is anything that is meant to be publicly known. There is no risk to anyone's privacy from you coming to know this.
- In public key cryptography
  - Public key
  - Private key (actually SECRET!)

Private information

- Your name is private.
  - It is not public information.
  - In closed environments such as a corporate office or a conference, your name is meant to be shared within that group, which is why you have to wear a name tag.
- An email or WhatsApp message you send to someone is private (similar to letters).
  - Other people cannot see it, unless you or the recipient choose to share it
  - Email and WhatsApp forwards are commonplace. They are still private.
    - There is no way to tell which piece of fake news is circulating around India on WhatsApp, because it’s private. You can only see what you send and receive.
    - Unless it somehow gets published in the media or on a public website, at which point it becomes public.

Where do we place Biometrics

- Our biometrics are also private information.
  - They are not secrets. You leave a copy of your fingerprints on almost everything you touch. Your iris biometrics can be extracted from a high resolution picture of your face, which even a modern smartphone is capable of. Unless you spend your life wearing gloves and shades, there is no hope of your biometrics being secret. They are available to the people you encounter in daily life, just like your name is.
- **Unlike your name**, other people have no use for your biometrics and don't pay attention to them, so we may be fooled into thinking they are secrets. They are not.
- Biometrics are not public either. There is no public database from which biometrics can be freely downloaded

What is privacy

- Privacy is about the responsible maintenance of private information. This responsibility is hard to define, which is why laws are necessary.

Private versus secret

Yiur Aadhar Number

- **Private,**
- **Neither secret nor public**

- Biometric Issues:
- Biometric matching gives probabilistic, not deterministic answers. That means the scanner will score your match on a scale of 0% to 100%. It cannot give a straightforward ‘yes’ or ‘no’ answer.
- Most Biometrics have been broken

Biometric Issues

- Biometric matching gives probabilistic, not deterministic answers. That means the scanner will score your match on a scale of 0% to 100%. It cannot give a straightforward ‘yes’ or ‘no’ answer.
- Most Biometrics have been broken

Authority versus authentication

Biometric at say Immigration:
When you arrive at a foreign destination (or a foreigner arrives in India), the immigration official at the counter decides whether to let you in. The fingerprint scanner on the desk informs this official. The official is the authority, not the scanner or some remote server.

Biometric at Aadhaar: Implicit assumption that the official at the bank or mobile company cannot be trusted to certify your identity. The authority is with the Scanner/Server