Privacy issues in ID/locator

draft-nordmark-id-loc-privacy-00
Erik Nordmark
Zededa
Some background and history

- **IDEAS BoF**
  - Some privacy solutions were discussed
- **ATICK BoF proposal**
  - Privacy stated as important
- **Draft** is an attempt to trigger some more detailed discussion around privacy
  - Threats and not about solutions
My Assumption in the draft

- Endpoints could have many and ephemeral identifiers with non-linkability properties
- Some sessions might want to survive mobility and multihoming events. Need an identifier which survives
- Thus focus on a single long-lived identifier
  - Ephemerals could improve things but can’t be the only answer
Some observations

● Why id/loc and exposing locators
  ○ Latency, bandwidth, autonomy/fault isolation

● Who and when?
  ○ OK? to expose IP location to friend while streaming video efficiently; not at other times or to other people
  ○ OK? to expose route optimization within autonomous system - similar to routing protocol
  ○ OK? For asset owner to track their trucks/machines
Different privacy threats

- **Location privacy**
  - Observer can determine the current IP locators
  - From packet?
  - By asking the mapping system?

- **Movement (event) privacy**
  - Observer can tell that identifier moved at time T
  - Can be correlated with other info (video, motion sensors) to determine who and where
Next steps?

- ID/loc system can be used improve location privacy (Tom Herbert)
  - Use a fixed anchor point locator
  - Less revealing than IP addresses as you move
  - Implies increased latency and more infrastructure dependency

- Who want to contribute?