Principles for Web and Networks solutions

Key characteristics for information exchange mechanisms between the Web Applications and Network layer

Dan Druta, AT&T **Web&Networks Interest Group 07/31/2019**

Privacy and Transparency

- Avoid passive interception and prevent man in the middle attacks
- Allow the client(user) and the server(content provider) to negotiate what and whom they want to give(or not) visibility into their flows
- User controlled privacy - this should be more than just relying on the user agent to automatically set privacy rules
- Minimize the fingerprinting entropy to avoid user tracking and long lived sticky identification of device, data flows or users

Trust

- Avoid solutions that rely on explicit trust relationships between parties as they tend to depend on sophisticated authentication infrastructures that are difficult to maintain
- Cheat-proof mechanisms based on trade-offs discourage parties to communicate misleading info are encouraged
- No guarantees expectation should be made in the process of bidirectional data exchange between network layer and web apps as there is no way to enforce these mechanisms across the Open Web Platform and all the network operators. Applications should not rely on or expect networks to always provide status info and vice versa

Data Integrity

- The only guarantee required for solutions should be on data integrity
- Encapsulation of data exchange should allow intermediaries in the path add info without tempering with existing flows

Focus on HINTS

- Solutions that provide hints to and from the network layer in order for the Apps to inform and be informed on:
  - Network conditions
  - Network access availability
  - Technology support (radio, etc.)