Privacy BCP
draft-cooper-ietf-privacy-requirements-01

Alissa Cooper
Stephen Farrell
Sean Turner

IETF principles in support of security and privacy

- **RFC 1984** encourages encryption
- **RFC 3365** requires strong security
- **RFC 2804** disallows consideration of wiretapping requirements
- **RFC 3552** guides consideration of security in protocol design
- **RFC 6973** guides consideration of privacy in protocol design

Development of further IETF consensus that:

- our protocols be designed to avoid privacy violations to the extent possible
- pervasive surveillance is an attack on privacy that should be defended against through protocol design

Personal data

- Definition: “Any information relating to an individual who can be identified, directly or indirectly.” (RFC 6973)
- Includes identifiers such as IP addresses that can remain consistent over time or that particular parties associate with directly identifiable information (such as a real name or street address)

Core proposed BCP text

To the extent consistent with basic protocol operation and management, standards-track IETF protocols that involve transmission of personal data:

1. MUST minimize their use of such personal data, and
2. where personal data is sent, MUST have well-defined and interoperable ways to send such data encrypted for the intended recipient(s).

Further articulation of (2)

- At minimum, opportunistic encryption MUST be well-defined for new IETF standards track protocols.
- Requirement can be waived only in exceptional circumstances where the protocol's utility would be eliminated or severely diminished if opportunistic encryption were defined.

End