Lessons from RFC 6973
Why did we write RFC 6973?

• Security as an IETF design consideration (RFC 1543, 2223, 3552, 3365, …)
  – Realistically cannot design and standardize a new protocol without confidentiality, authentication, integrity, etc. protections or strong story for why not.

• Recognition within IAB and IETF of privacy as a design consideration.
How did we write RFC 6973?

- Individual informational draft first published in 2010.
- IAB Privacy (now Privsec) program took it up 1 year later.
- Published in IAB stream July 2013.
- Retained significant content from individual draft and structure from RFC 3552.
(Hard-fought) decisions (1/2)

• Limited ambition, general applicability
  – No definition of “privacy.”
  – No explicit prohibitions or requirements.
  – No required privacy considerations section.
  – No specific legal framework.

• Acknowledged scope limitations
  – What can be addressed in protocol design vs. deployment and operation.
  – What can be addressed at each network layer.
(Hard-fought) decisions (2/2)

• Made distinction between (negative) defending against exploits and (positive) building privacy tools.

• Provided specific examples.
If you write an RFC in a forest, will anybody read it?

• Privacy tutorials – ~3 in 2013-14
• Privacy directorate – could not sustain
• Other activities and ideas
  – Reviews of old RFCs
  – Privacy expertise in IESG criteria for nomcom
  – Incorporating bits of RFC6973 into a RFC3552bis
  – Refresh of tutorial, record for later consumption
Results
Results

• Privacy awareness has increased among protocol designers.
  – Demonstrated in many docs arriving for IESG review (and published).

• Specific checklist only occasionally used (extreme example: RFC 7594).

• Attention to privacy still highly dependent on authors, last call/secdir reviewers, ADs who happen to be there at the time.

• Deployment of more privacy-friendly features/protocols also clearly on the rise.
Thoughts about human rights considerations in protocol design

• Focus on one area at a time
  – Censorship resistance? Decentralization?

• Focus on areas lacking in guidance
  – Security, privacy, internationalization, extensibility all well-trod already

• Provide specific examples of application
  – If an existing protocol design had considered X, how would it have changed?

• Be specific about scope limitations
  – Protocol vs. implementation vs. deployment
  – Upper layers vs. lower layers