

Moves and counter-moves in IETF RFCs about user surveillance

Stéphane Bortzmeyer

Afnic

1 october 2026

Context: what is IETF

- Internet Engineering Task Force standardizes Internet protocols (IP, DNS, BGP, HTTP, etc)
- “Between layer 3 and (partially) layer 7”
- International organisation
- No official role, not a regulator
- “There is no IETF police”
- Just a moral authority
- A galaxy of related organisations (IAB, IRTF, etc)

Context: RFC

- The acronym meant something but no longer
- Important texts, including technical standards
- Each has a number
- Various streams (not all of them IETF)
- Not all RFC are standards

Context: the culture

- IETF originated in a technical world in the USA
- Often described as very privacy-conscious and fan of individual freedom
- Also marked by the old idea that technical standards are neutral
- But it is more complicated than that
- Technical operators need some level of surveillance
- Some protocols raise privacy issues: should we standardize things that could be used for bad?

Before consciousness

- RFC 1635 “How to Use Anonymous FTP”
- May 1994
- Not anonymous at all
- “Traditionally, this special anonymous user account accepts any string as a password, although it is common to use either the password “guest” or one’s electronic mail (e-mail) address.”

First time IETF had to stand

- August 1996
- RFC 1984 “IAB and IESG Statement on Cryptographic Technology and the Internet”
- IAB: long-term architecture board, IESG: technical direction of the IETF
- “Crypto wars”: the RFC rejects the idea of backdoors and argues for strong crypto

Snowden

- RFC 6973 “Privacy Considerations for Internet Protocols”, first comprehensive analysis of the role of technical protocols in making tracking easier or more difficult
- Issued by IAB
- July 2013
- RFC 7258 “Pervasive Monitoring Is an Attack”, promises to work against pervasive surveillance
- Issued by IETF
- May 2014

Stable identifiers considered harmful for privacy

- RFC 7844 “Anonymity profile for DHCP clients”
- RFC 7819 “Privacy considerations for DHCP”
- April/May 2016

Human rights is now a subject

- RFC 8280 “Research into Human Rights Protocol Considerations” (not only privacy)
- Issued by IRTF (the R&D arm)
- October 2017

But not everyone agrees

- RFC 8404 “Effects of Pervasive Encryption on Operators”
- IETF but not a standard
- July 2018
- A plea for the ability to track/watch users and their activity
- Operational reasons
- See also the drama about DoH, RFC 8484 “DNS Queries over HTTPS”

Two famous fights

- RFC 8446 “The Transport Layer Security (TLS) Protocol Version 1.3”, encrypts more stuff
- August 2018
- Very long fight about “visibility” for the network operators
- RFC 9000 “QUIC: A UDP-Based Multiplexed and Secure Transport”
- May 2021
- The spin bit, the most contentious bit of the Internet