Privacy Reviews for Internet and Web Standard-Setting

The Standards Process

The World Wide Web Consortium and the Internet Engineering Task Force provide the context for Web and Internet standards conversations, though alternative and competing fora exist. But how do we identify and address privacy issues in these fundamental standards?

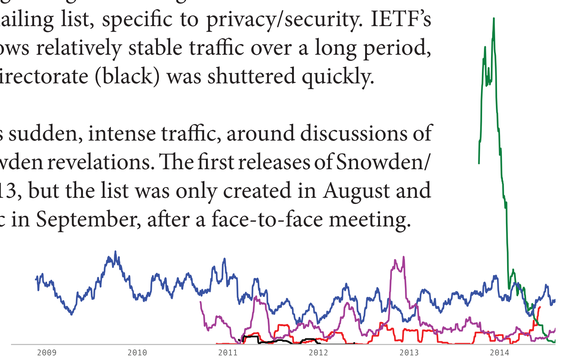
These standard-setting organizations follow a multistakeholder model familiar to Internet governance. Decisions are made by "rough consensus and running code" and adoption of standards is voluntary. However, both organizations have process and hierarchy; for example the Area Directors at IETF and the Director (Tim Berners-Lee) at W3C exercise judgment over whether specifications advance to standardization.

"the Security Area Directors are a force to be reckoned with"

The work — discussion, debate, iteration on solutions — of technical standard-setting is done at face-to-face meetings (in conference rooms, see the photo of a W3C Working Group meeting at the Berlaymont in 2012) and, more significantly, via mailing lists, which provide an extensive corpus for study.

These lines compare the moving average of mailing list traffic on several IETF mailing lists, and one W3C mailing list, specific to privacy/security. IETF's Security Directorate (blue) shows relatively stable traffic over a long period, while the attempted Privacy Directorate (black) was shuttered quickly.

In green, the **perpass** list shows sudden, intense traffic, around discussions of IETF's response to various Snowden revelations. The first releases of Snowden/NSA documents were June 2013, but the list was only created in August and started seeing significant traffic in September, after a face-to-face meeting.



IETF/W3C non-Working Group, privacy/security mailing list traffic

For links to literature and tools mentioned in this poster, see: https://npdoty.name/tprc42

How to Study Standard-Setting

As part of a larger ethnographic study of standard-setting, I'm using the following methods for *polymorphous engagement* with these multistakeholder processes.

Semi-Structured Interviews
Interviews with participants (including engineers, advocates and regulators) in standard-setting processes provide a thick, emic account of the process. Quotes throughout this poster come from initial interviews with IETF participants.

Mailing List Analysis
Berkeley researchers are currently developing **BigBang**, a suite of open source Python software for performing automated text and network analysis of mailing lists. We expect this to be particularly useful for studying software development and Internet governance communities.

Documents and Software
We also have a rich corpus of the published standards themselves, as well as software implementations.

Initial Analysis of Trends

Systematizing Privacy Reviews
including the development of guidance documents: *RFC 6973*, *Specification Privacy Assessment* and *Fingerprinting Guidance for Web Specification Authors*.

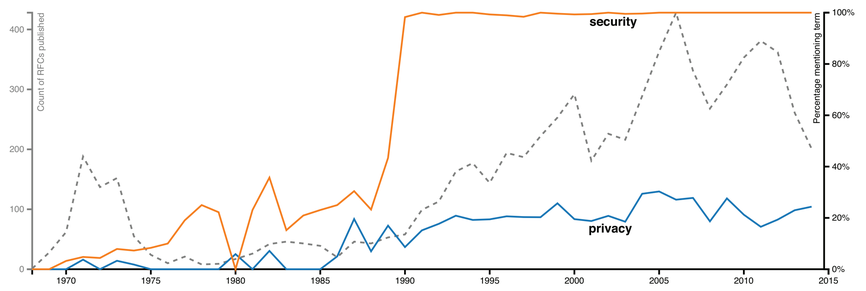
"because right now it's very ad hoc"

Integration of Security and Privacy
coordination of reviews for surveillance, security and privacy issues; combination into IAB Privacy & Security Program.

"security is bleeding over into privacy"

Process Requirements
in some (but not all) cases, leadership roles or process requirements make a difference.

Privacy in Published Standards

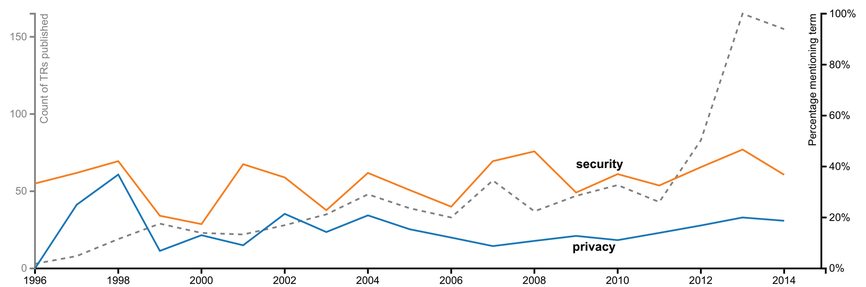


Percentage of published IETF RFCs with search terms, by year

In dashed grey (left axis), the number of RFCs published each year, from 1969 until 2014. In orange and blue, the fraction (right axis) of that year's RFCs that have at least a single mention of the terms "security" or "privacy", a naive metric. Compliance with the requirement for security considerations seems to be near complete, mentions of "privacy" seem to level off at a fifth of all the documents published. The presence of a "Security Considerations" section doesn't guarantee a sound security review and privacy may be present in a technical design without any mention of the term. See:

Braman, Sandra. "Privacy by Design: Networked Computing, 1969–1979." *New Media & Society* 14, no. 5 (August 2012): 798–814.

Rabkin, Ari, Nick Doty, and Deirdre K Mulligan. "Facilitate, Don't Mandate." *IAB/W3C Internet Privacy Workshop*. 2010.



Percentage of W3C Technical Reports with search terms, by year

In dashed grey (left axis), the number of TRs published each year, from 1996 until 2014. In orange and blue, the fraction (right axis) of that year's TRs that have at least a single mention of the terms "security" or "privacy", a naive metric. As the number of documents increases, the relative mentions of security and privacy have remained roughly stable.

Nick Doty • https://npdoty.name
npdoty@ischool.berkeley.edu
UC Berkeley School of Information