Reviewing for privacy in Internet and Web standard-setting

Nick Doty
UC Berkeley, School of Information

Outline

1. Internet standards at IETF & W3C

2. History of security and privacy reviews

3. Reactions to Snowden

4. Future directions

W3C Recommendation

HTML5

A vocabulary and associated APIs for HTML and XHTML

W3C Recommendation 28 October 2014

This Version:
http://www.w3.org/TR/2014/REC-html5-20141028/
Latest Published Version:
http://www.w3.org/TR/html5/
Latest Version of HTML:
http://www.w3.org/TR/html/
Latest Editor's Draft of HTML:
http://www.w3.org/html/wg/drafts/html/master/
Previous Version:
http://www.w3.org/TR/2014/PR-html5-20140916/
Previous Recommendation:
http://www.w3.org/TR/1999/REC-html401-19991224/
Editors:

WHATWG:
Ian Hickson, Google, Inc.
W3C:
Robin Berjon, W3C
Steve Faulkner, The Paciello Group
Travis Leithead, Microsoft Corporation
Erika Doyle Navara, Microsoft Corporation
Edward O'Connor, Apple Inc.
Silvia Pfeiffer

3.2.6. Field Value Components

Most HTTP header field values are defined using common syntax components (token, quoted-string, and comment) separated by whitespace or specific delimiting characters. Delimiters are chosen from the set of US-ASCII visual characters not allowed in a token (DQUOTE and "(),/:;<=>?@[\]{}").

```
  token          = 1*tchar

  tchar          = "!" / "#" / "$" / "%" / "&" / "'" / "*"
                 / "+" / "-" / "." / "^" / "_" / "`" / "|" / "~"
                 / DIGIT / ALPHA
                 ; any VCHAR, except delimiters
```

A string of text is parsed as a single value if it is quoted using double-quote marks.

```
  quoted-string  = DQUOTE *( qdtext / quoted-pair ) DQUOTE
  qdtext         = HTAB / SP /%x21 / %x23-5B / %x5D-7E / obs-text
  obs-text       = %x80-FF
```

Comments can be included in some HTTP header fields by surrounding the comment text with parentheses. Comments are only allowed in fields containing "comment" as part of their field value definition.

```
  comment        = "(" *( ctext / quoted-pair / comment ) ")"
  ctext          = HTAB / SP / %x21-27 / %x2A-5B / %x5D-7E / obs-text
```

The backslash octet ("\") can be used as a single-octet quoting mechanism within quoted-string and comment constructs. Recipients that process the value of a quoted-string MUST handle a quoted-pair as if it were replaced by the octet following the backslash.

```
  quoted-pair    = "\" ( HTAB / SP / VCHAR / obs-text )
```

A sender SHOULD NOT generate a quoted-pair in a quoted-string except where necessary to quote DQUOTE and backslash octets occurring within that string. A sender SHOULD NOT generate a quoted-pair in a comment except where necessary to quote parentheses ["(" and ")"] and

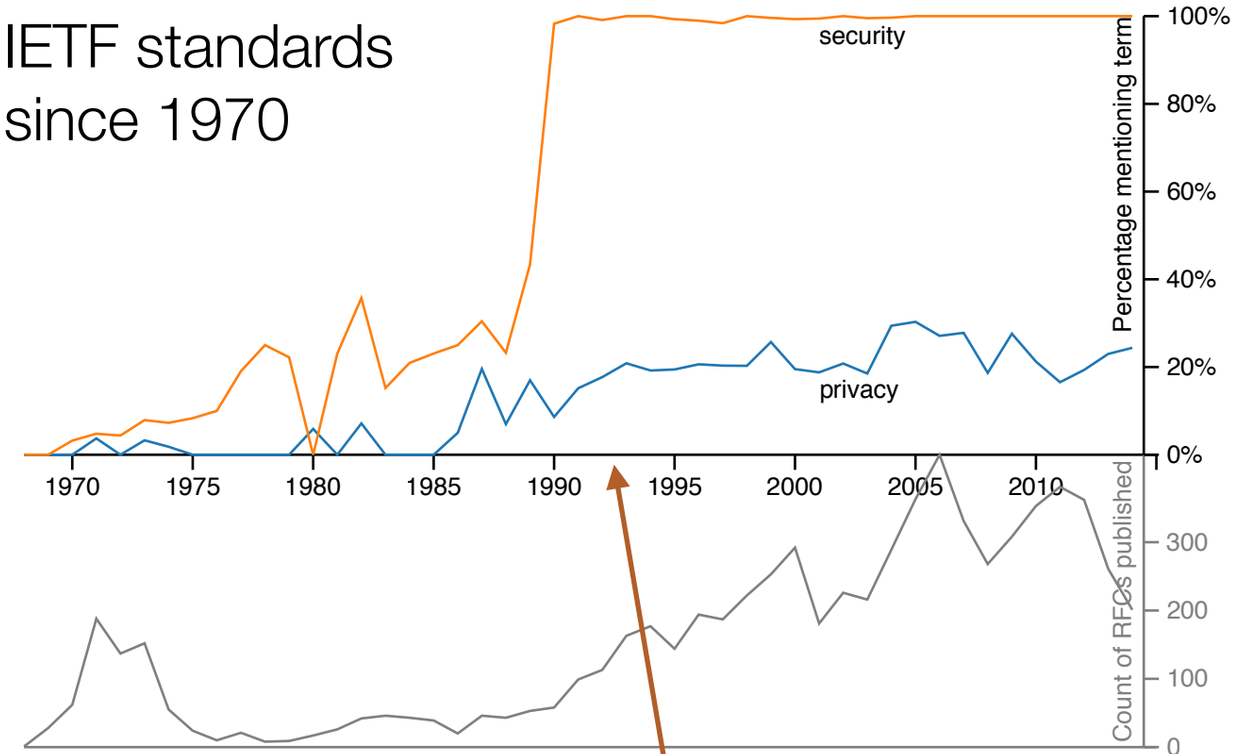
What is a standard?

- [perpass] What problems does perpass need to solve?, *Dave Crocker*
  - Re: [perpass] What problems does perpass need to solve?, *Randy Bush*
    - Re: [perpass] What problems does perpass need to solve?, *Dave Crocke*
      - Re: [perpass] What problems does perpass need to solve?, *Tim Br*
      - Re: [perpass] What problems does perpass need to solve?, *Eduard*
      - Re: [perpass] What problems does perpass need to solve?, *Leif Jo*
      - Re: [perpass] What problems does perpass need to solve?, *Stephe*
      - Re: [perpass] What problems does perpass need to solve?, *Leif Jo*
      - Re: [perpass] What problems does perpass need to solve?, *Alissa*
      - Re: [perpass] What problems does perpass need to solve?, *Scott B*
  - [perpass] HTTP user-agent fingerprinting, *Patrick Pelletier*
    - Re: [perpass] HTTP user-agent fingerprinting, *Stephen Farrell*
      - Re: [perpass] HTTP user-agent fingerprinting, *Patrick Pelletier*
      - Re: [perpass] HTTP user-agent fingerprinting, *Roy T. Fielding*
      - Re: [perpass] HTTP user-agent fingerprinting, *Poul-Henning Kan*
      - Re: [perpass] HTTP user-agent fingerprinting, *Martin Thomson*
      - Re: [perpass] HTTP user-agent fingerprinting, *David Morris*
      - Re: [perpass] HTTP user-agent fingerprinting, *Karl Dubost*
      - Re: [perpass] HTTP user-agent fingerprinting, *William Chan (陈智*
      - Re: [perpass] HTTP user-agent fingerprinting, *Randy Bush*
      - Re: [perpass] HTTP user-agent fingerprinting, *Yoav Nir*
      - Re: [perpass] HTTP user-agent fingerprinting, *George Michaelso*
      - Re: [perpass] HTTP user-agent fingerprinting, *Yoav Nir*
      - Re: [perpass] HTTP user-agent fingerprinting, *Randy Bush*
      - Re: [perpass] HTTP user-agent fingerprinting, *Nicolas Mailhot*
      - Re: [perpass] HTTP user-agent fingerprinting, *Karl Dubost*
      - Re: [perpass] HTTP user-agent fingerprinting, *Nicolas Mailhot*
      - Re: [perpass] HTTP user-agent fingerprinting, *Scott Brim*
    - <Possible follow-ups>
    - Re: [perpass] What problems does perpass need to solve?, *Dickson, Brian*
- Re: [perpass] [TLS] Let's remove gmt_unix_time from TLS, *Peter Gutmann*
- Re: [perpass] [TLS] Let's remove gmt_unix_time from TLS, *Peter Gutmann*
  - Re: [perpass] [TLS] Let's remove gmt_unix_time from TLS, *Marsh Ray*
- [perpass] PRISM-Proof Criteria, *Phillip Hallam-Baker*
  - *Message not available*
    - Re: [perpass] PRISM-Proof Criteria, *SM*

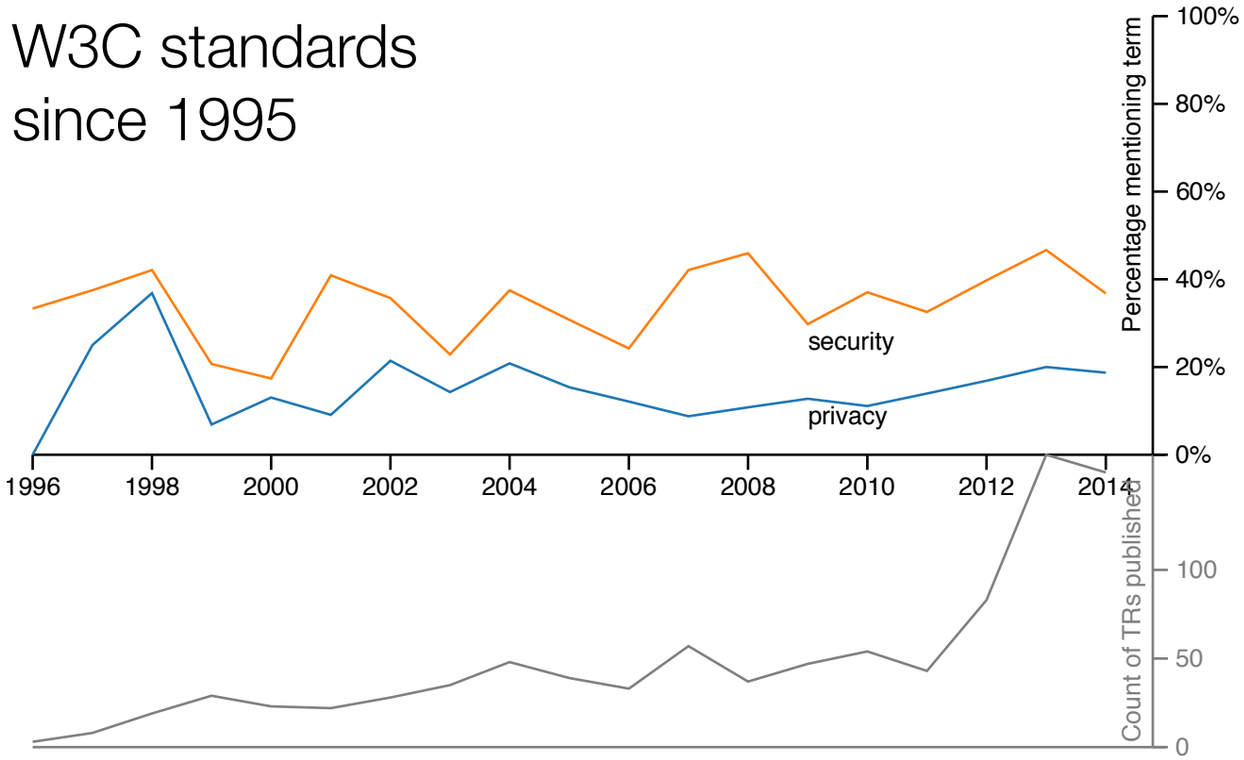
Making standards

Privacy and security in standards over time

IETF standards
since 1970



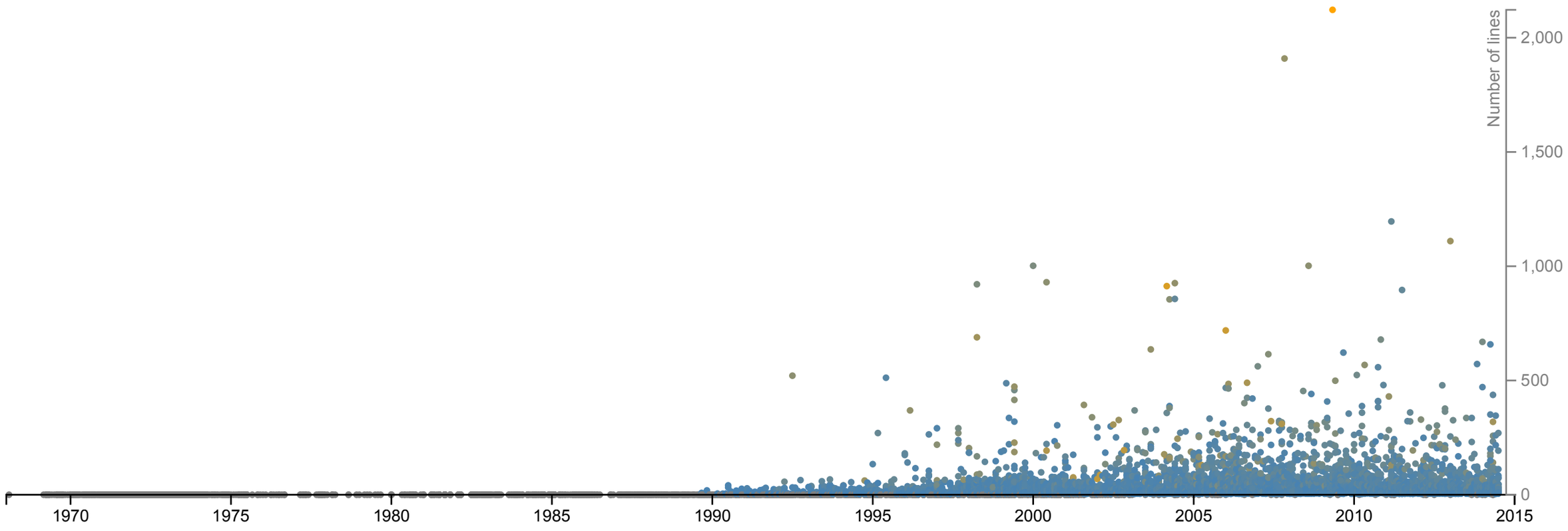
W3C standards
since 1995



1993: “Security Considerations” section required

Substantivity of “Security Considerations”

All RFCs are required to have a Security Considerations section. Historically, such sections have been relatively weak.
—RFC 3552 (2003)



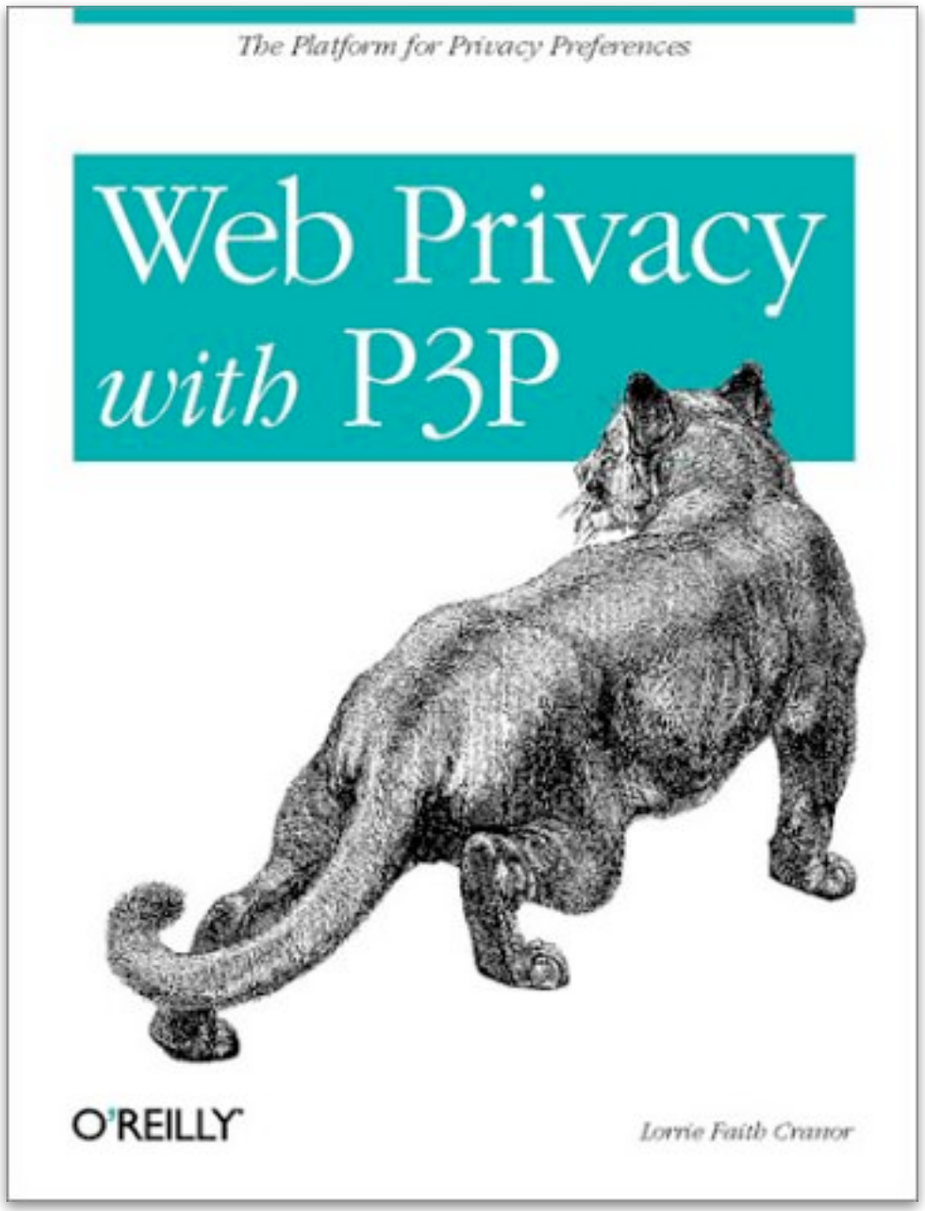
Leadership and systematization

"Now everyone [thinks about security]. Not everyone does, but as soon as you don't, you get called out. […] The security area directors are like a force to be reckoned with at this point.

Free lunches got a volunteer Security Directorate started. "Once it was institutionalized and organized, [...] there was enough momentum to keep it going."

interviews with IETF participants

Privacy-specific Web standards



DNT: 1

Tools for privacy and security reviews

- RFC 3552: Guidelines for Writing RFC Text on Security Considerations
- RFC 6973: Privacy Considerations for Internet Protocols
- Self-Review Questionnaire: Security and Privacy
- Fingerprinting Guidance for Web Specification Authors
- Specification Privacy Assessment

Snowden reactions

- From individuals:

we had a good thing

you messed it up

for everyone

we trusted you

we were naive

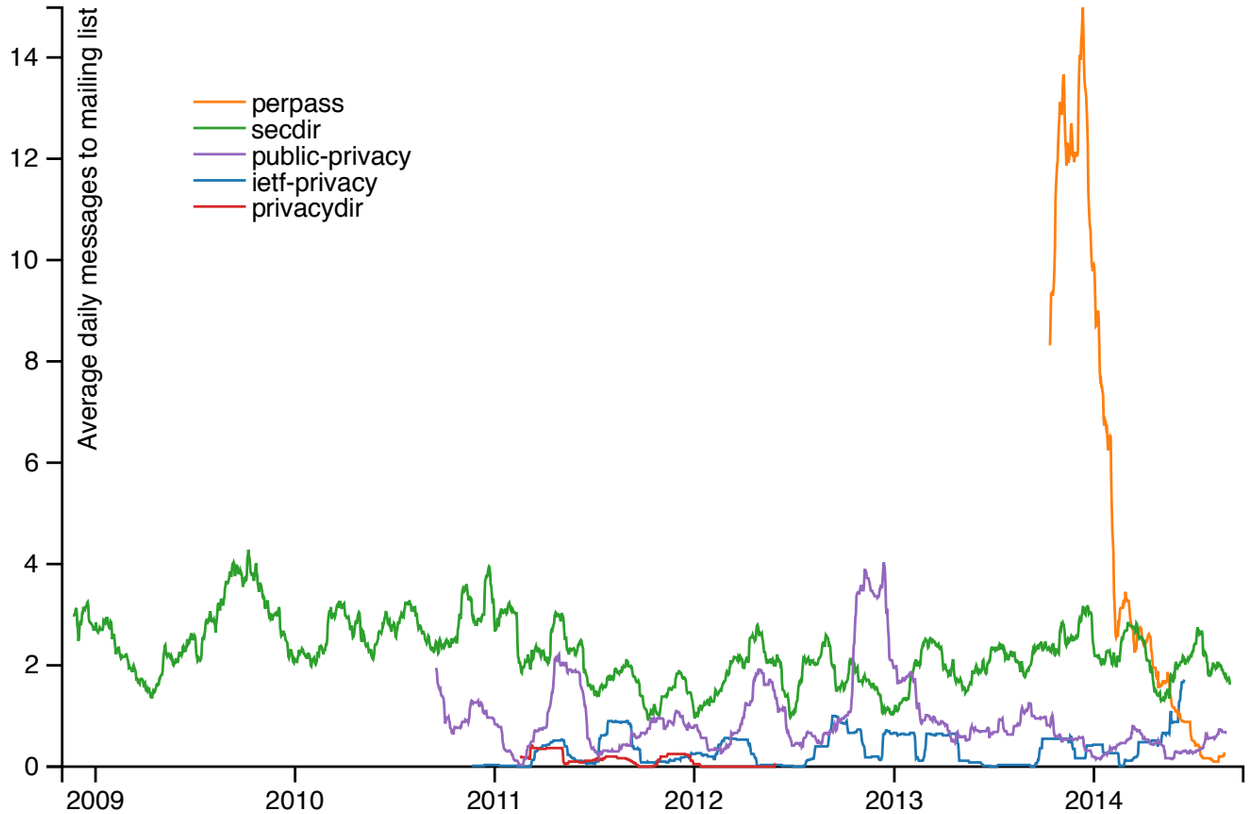
never again

Thomson, Martin. 2013. A Simple Statement. http://www.ietf.org/internet-drafts/draft-thomson-perpass-statement-00.txt.

Aymann Ismail/ANIMALNewYork

Snowden reactions

- From groups:



Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Farrell, S, and H Tschofenig. 2014. Pervasive Monitoring is an Attack. RFC 7258. RFC Editor. http://tools.ietf.org/html/rfc7258.

Groups for privacy and security reviews

- W3C Privacy Interest Group
- Web Security Interest Group
- W3C Technical Architecture Group
- IETF Security Directorate
- perpass (*per*vasive *pas*sive surveillance)
- IAB Privacy & Security Program

Future work

- What tools are effective and how can a systematized process be set up in a standard-setting environment?
- What can we learn about consideration of values (privacy, security, accessibility, freedom of expression) in multistakeholder groups?

Thanks!

Nick Doty
npdoty@ischool.berkeley.edu
https://npdoty.name