Privacy Reviews in PING

Or, How to Lose Friends and Influence Privacy
(kidding…)

Pete Snyder, PING Co-Chair (pes@brave.com - Brave Software - @pesk10)

Privacy Reviews in PING
Outline

- **What Are Privacy Reviews:**
  Why, when and who

- **Goals of Privacy Reviews:**
  What becomes who's problem

- **Conducting the Privacy Review:**
  What to expect when you're expecting privacy

- **Conclusion**

Privacy Reviews in PING
Outline

- **What Are Privacy Reviews:**
  Why, when and who

- **Goals of Privacy Reviews:**
  What becomes who's problem

- **Conducting the Privacy Review:**
  What to expect when you're expecting privacy

- **Conclusion**

What Are Privacy Reviews

- Part of W3C process to:

  1. Address privacy issues in specs, to ease compatibility in implementations

  2. To uphold ethical design principals and web constituency priorities

- Part of Horizontal Review

  1. Accessibility

  2. Internationalization

  3. Privacy

What Are Privacy Reviews

- Privacy Reviews and Spec Lifetimes

  - Privacy (and all) reviews are done before moving to rec

  - Can also be requested

- Some issues

  - Relationship to TAG reviews

  - Causes fights; most implementation work is done already

  - This process may change

What Are Privacy Reviews
Example Timeline

- Working group (WG) wants to move to Rec

- WG announces, and requests HR reviews

- At least one <u>PING member is assigned</u> to do the review

- Reviewer discusses with PING

- Issues are filed in WG repo, echoed in <u>PING tracking-issues repo</u>

- Iteration and discussion with WG to address

- Escalate to formal objections if needed (rare)

Privacy Reviews in PING
Outline

- **What Are Privacy Reviews:**
  Why, when and who

- **Goals of Privacy Reviews:** ⟵
  What becomes who's problem

- **Conducting the Privacy Review:**
  What to expect when you're expecting privacy

- **Conclusion**

Goals of Privacy Reviews
Definitely In Scope

- Identifying new harms in new spec functionality

- Identifying existing harms in existing spec functionality ("technical debt")

- Identifying where spec is not "privacy by default"

  - Protections are suggested / not-required / non-normative / left to implementors

  - Included protections require additional steps

Goals of Privacy Reviews
Definitely Not In Scope

- PING Redesigning specs to achieve WG goals in a privacy-way

- Accepting responsibility for WG expertise
  (i.e. PING should do a study… then we'll change it)

- Making "functionality vs privacy" trade-offs

- Philosophical arguments about the value / necessity of privacy

- Writing spec text

- Privacy reviews being used to add non-privacy functionality

Goals of Privacy Reviews
Reviewers / PINGs discretion

- Assisting the WG group on alternative solutions

- Providing existing research demonstrating the problem

- Connecting the WG with privacy folks who could help with the above

Goals of Privacy Reviews
Overall Though

- Focus on collaboration; no one has to do any of this!

- Focus on the joint goal of improving the web

- Keep in mind the long term impact of privacy decisions made today!

Privacy Reviews in PING
Outline

- **What Are Privacy Reviews:**
  Why, when and who

- **Goals of Privacy Reviews:**
  What becomes who's problem

- **Conducting the Privacy Review:**
  What to expect when you're expecting privacy

- **Conclusion**

Conducting A Privacy Review

- **Pre-Review:**
  How is it requested, assigned, committed to

- **Doing the Review:**
  High level suggestions for doing a review

- **After the Review:**
  Sharing the results of a review

Conducting A Privacy Review
Pre-Review Steps

- PING gets request for a review (e.g., <u>public-privacy@w3.org</u>)

- Agree to do a review, notify the PING Co-Chairs

- Create privacy review issue
  <u>https://github.com/w3cping/tracking-issues</u>

- Communicate expected timeline with WG and PING

Conducting A Privacy Review
Conducting the Review

1. Understand goals and functionality of spec

   • Spec text

   • Explainers

   • Asking others in PING

   • Asking the WG

Conducting A Privacy Review
Conducting the Review

2. Issues to look for

- New explicit state

- New implicit state (fingerprinting surface)

- Accidental or unneeded information disclosure

- How are the above constrained / limited / restricted

- The private path exists, but isn't default

- Non-normative "fixes"

Conducting A Privacy Review
Conducting the Review

3. Guiding Questions

- Does the default spec behavior harm privacy?

- Could the spec make it more difficult to solve other, existing privacy harms?

- Is the user always centered?

- Are there foot-guns (and of what caliber?)

Conducting A Privacy Review
Completing the Review

- Discuss review findings on next PING call

- File issues in WG's repos

  - **"privacy"**
    Issue impacts privacy and the WG should look into it

  - **"privacy needs review"**
    The above, but enough that the spec should not proceed without fixing

  - Issues are mirrored in PING's tracking issues repo

- Notify WG of the review and issues

Privacy Reviews in PING
Outline

- **What Are Privacy Reviews:**
  Why, when and who

- **Goals of Privacy Reviews:**
  What becomes who's problem

- **Conducting the Privacy Review:**
  What to expect when you're expecting privacy

- **Conclusion**

Conclusions and Suggestions
Privacy Reviews…

- have been successful in improving privacy on the platform

- are exhausting, and sometimes combative

- sometimes emotionally draining

- require significant understanding of the web platform, but thats insufficient

- are worth the time; they often yield material, concrete improvements

Conclusions and Suggestions

- You don't have to do it alone!

- Abusive behavior isn't acceptable

- ABD (always be depersonalizing)

- Appreciate the WG's work

- Escalate when necessary

- Focus on long term goal of improving the Web