WebRTC: User Security & Privacy

W3C TPAC
Anant Narayanan, Mozilla

October 31, 2011

Overview

- Placement in standard
- Behavior on getUserMedia()
- Immediate & long-term permissions
- Permissions & user model
- User privacy indicators
- Summary

Placement in Standard

- We currently do not specify what happens when getUserMedia is called with regards to asking user permission

- Such a specification may not fit in the standard as user agents vary wildly

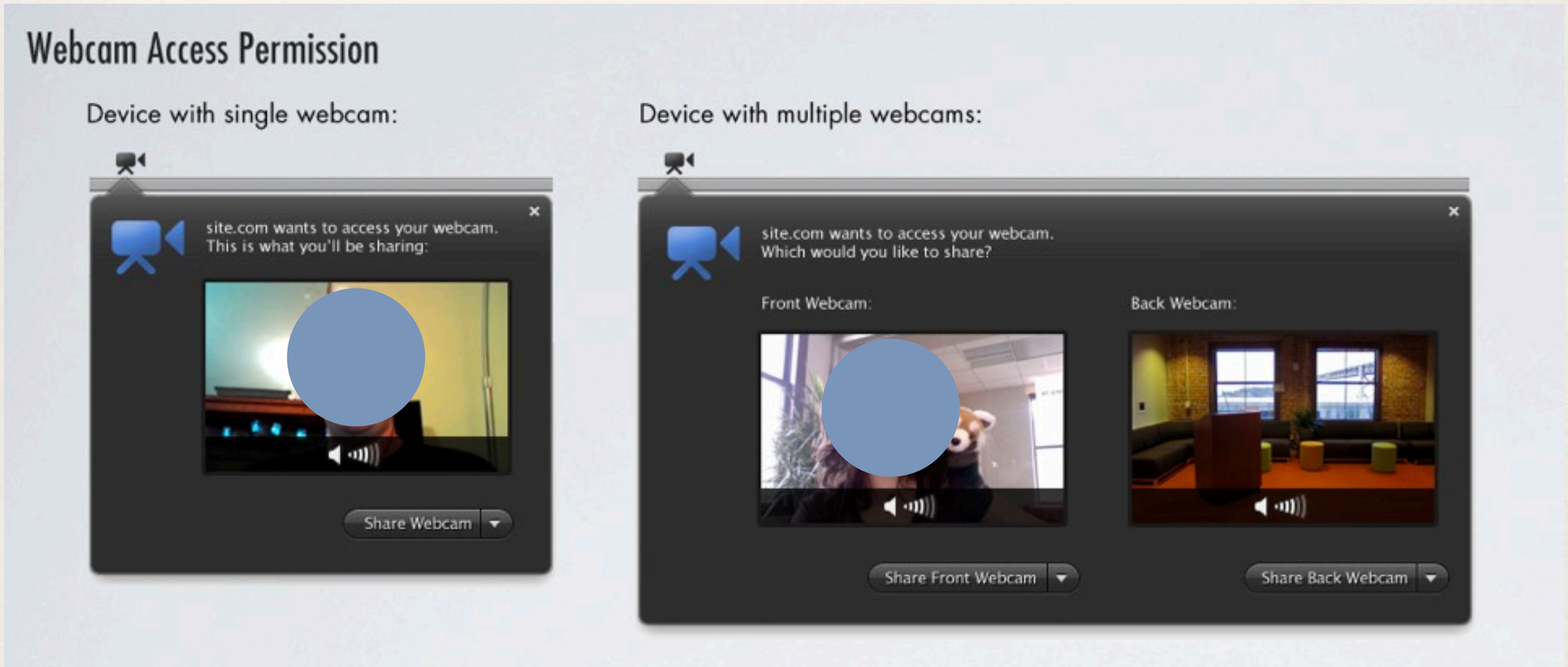
- We can, however, come up with a set of “recommended guidelines” for major browser vendors to adopt (a specific type of a user agent)

- Open question: Is the W3C spec the right place to put this?

User Permission

- getUserMedia() is asynchronous to allow the UA to ask the user permission, and choose exactly what media gets shared:
  - Video from webcam(s)
  - Audio from microphone(s)
  - Transmit A/V from local media files
- Give user complete control over what is transmitted, irrespective of what the web application asked for

Early Mockup



Details…

- Firefox “Doorhanger”, distinguishes a browser request from regular web content and is a trusted space
  - Somewhat harder to spoof than an infobar (not really, just 2px!)
- If application asked for both audio and video, default to both but allow user override (not depicted)
  - Front/Back camera preferences better handled as “hints”?
- A list of granted permissions is always available and revocable from a “preferences” pane

Immediate & long-term

- What is the time period for which the user grants access?
  - Default is immediate (one-time only), user may explicitly choose "Always allow example.org to access A/V"
- Should the web-application be able to specify what type of access it needs?
- How are these permissions persisted?

Permissions & Sessions

- Initial proposal was to tie a permission grant to a time-frame and domain name

- Feedback from web developers:
  - Permissions should actually be tied to a user session, not just domain. Until everyone uses BrowserID, this means cookie jar?
  - More realistically, we could allow the application itself to “revoke” a granted permission if it detects a change in user session?

After permission is granted...

Notification in Tab

Summary

- Mostly a set of UI and interaction guidelines, may not be applicable to all user agents (or to varying degrees)

- Where do we write this stuff down?

- Other open questions:

  - What happens if devices are already in use by another application?

  - What is the interaction for an incoming call?