Effective Device API Privacy: Protecting Everyone (Not Just the User)

Susan Landau[1]

The html5 specifications for device APIs specify browser support for static images and video, and discuss the possibility of support for the capture of sound [1]. Such data acquisition has the potential to be highly privacy invasive. An accompanying *Device API Privacy Requirements* draft proposes various privacy protections, including that defining APIs be naturally privacy respecting, and empowering users so that they can express privacy preferences [3]. This document emphasizes the fair information practices of notice, consent, control, but all these protections are focused on the user's privacy. This misses a large aspect of the problem.

Unlike the capture of content by a digital camera or a cellphone — both of which are likely to be visible — the capture of video and/or sound content by a browser running on the user's desktop can be passive. The device sits and records. While the privacy protections embodied in the *Device API Privacy Requirements* may ensure that the device's owner has actively assented to recording, others in recording range will not necessarily have done so. Neither the html5 device API nor the accompanying privacy requirements address this concern.

User notice is simply inadequate in this situation. Indeed, by seeking to surreptitiously record others within range without their notice, the user may be the problem. Changing technology requires changing privacy practices, and replacing the taking of photographs with recording video and sound means an adjustment of privacy protections is in order. In particular, privacy protections need to be far more dynamic than the "user notice and consent" model currently being proposed in the *Device API Privacy Requirements.*

I propose that html5 device APIs include a "MUST" requirement that video or sound recording be accompanied by automatic flash or beeping occurring every fifteen seconds. Such light and/or noise will be disruptive to any within recording range, *but that is exactly the point.* Those who are being recorded should be made aware that recording is occurring.

There is precedent for such intrusive action. For example, in the U.K. the Data Protection Act requires that when Closed Circuit Television Cameras are used, "Signs should placed so that the public are [sic] aware that they

[1] Radcliffe Institute for Advanced Study, Harvard University

are entering a zone which is covered by surveillance equipment," and that these signs must be visible to the public[2]. The U.S. Federal Communications Commission requires that a recording party notify the other party of recording if a wireline call is interstate or international. Such recording must be preceded by verbal or written consent from all parties, by verbal notification that occurs during recording of the communication, or by an automatic beeping at regular periods during the call [2].

The specifications could allow for some user type of disablement of the flashing/beeping, but only if the disabling "MUST" were active. That is, the specification might allow disabling, but would require that after two minutes of uninterrupted recording, the flashing and/or beeping MUST restart, and any subsequent ceasing would require active user intervention. Such a refinement would limit disruptive flashing/beeping, but would still provide privacy protection to an otherwise unnotified public.

Exactly how to implement active notice will take some effort. But to protect privacy, it is imperative that video and sound recording be accompanied by active notice.

References

[1] Berjon, Robin, Daniel Coloma, Max Froumentin, Marcin Hanclik, Jere Käpyaho, Kangchan Lee, Bryan Sullivan, Dzung Tran, *Device APIs Requirements,* W3 Working Group Notes, 15 October 2009, http://www.w3.org/TR/dap-api-reqs.

[2] Consumer and Governmental Affairs Bureau, Federal Communications Commission, *Recording Telephone Conversations: FCC Consumer Facts,* Septemer 22, 2008.

[3] Cooper, Alissa, Frederick Hirsch, and John Morris, *Device API Privacy Requirements,* W3C Working Group Notes, 29 June 2010, http://www.w3.org/TR/dap-privacy-reqs.

[4] Information Commissioner, *CCTV Code of Practice 2008.*

[2] In addition, there are limitations on how long the data is to be kept and who is allowed access to the data [4, pp. 11-12].