UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

SCHOOL OF INFORMATION
102 SOUTH HALL # 4600
BERKELEY, CALIFORNIA 94720-4600
(510) 642-1464
(510) 642-5814 Fax

March 25, 2011

Web Tracking and User Privacy position paper

The W3C, the IETF, and other technical standard-setting bodies are poised to make a significant contribution to the development of scalable, technically-enabled approaches to privacy protection. Regulators, industry, advocates, and academics are looking to technical standards with renewed interest. The W3C should welcome the focus on the interplay between technical standards and social values and take this opportunity to fully enter the privacy conversation in a sustained and meaningful way.

Collaborative and non-collaborative filtering

Effectively protecting user privacy in the face of ubiquitous and invisible tracking on the Web will likely require multiple policy and technical solutions. The experience dealing with unsolicited commercial email (spam) is instructive. Multiple technical and policy approaches were required to reduce the burden spam places on end users and networks. Spam filters allow for both black and white listing, while legislation and self-regulatory approaches that require labeling facilitate collaborative filtering.

The current proposals to address tracking for online behavioral advertising map these two approaches. Microsoft's member submission proposes a list-based blocking system, as well as a technical expression of a user preference (a Do Not Track header and property). The blocking operates much like black-lists in spam filtering, providing protection without the cooperation of other entities. This offers an important form of pre-emptive protection where the marketplace is comprised of entities with varying motivations to abide by users' wishes whether backed by law or not. The Do Not Track header/property, in contrast, requires that receiving entities abide by the expressed preference in order for privacy to be improved. Pursuing both options will allow Web browsers to work in both collaborative and non-collaborative settings, potentially improving privacy both in cases of good actors (who respect expressed user preferences) and bad actors (who might ignore or lie about their practices). Of course, as has been well-documented, the "arms race" of new tracking methods (HTTP cookies, Flash cookies, browser history sniffing, and on and on) suggests that tracking protection lists will not be the last necessary technical method for blocking tracking, nor need it be. In the same way, Do Not Track and other user privacy expressions may evolve beyond a single binary option.

The need for a multi-stakeholder process

As illustrated by the technical proposals to address behavioral advertising, addressing privacy concerns requires coordination with non-technical parties and respect for the distinct spheres of expertise all participants bring to the discussion. The W3C's past experience with specifications within the technology and society domain suggest that a successful effort requires: 1) full participation of the

entities that must implement all aspects of the specification; 2) structures to maximize the ability of non-technical stakeholders with relevant privacy expertise to participate in appropriate elements of the specification; and, 3) participation that is geographically diverse to ensure technical interoperability despite competing policy approaches.

As with spam, the definition of the prescribed behavior — tracking — is not purely technical. Crafting the definition of tracking will require non-technical input. It may, as with the P3P vocabulary, argue for the creation of a separate expert group. Such an expert group should be broadly representative of the stakeholders and attentive to the need for responses that address varied global regulatory approaches. Technical approaches will be most useful if they support regional variations in privacy. A Do Not Track specification would be most useful if it interacts supportively with the ePrivacy Directive and opinions of the Article 29 Working Group as well as whatever regulatory and self-regulatory approaches emerge in the US and other countries. As in accessibility and P3P, precedent suggests that separating (but coordinating) technical and policy definitions can remove friction from the development process and leave flexibility where policy demands it.

Technical standards and privacy by design

Focused work on the issue of behavioral advertising provides an opportunity to make an important contribution to a pressing public policy concern. However, privacy needs sustained attention. The current proposals to address behavioral advertising, like P3P before it, are episodic and largely reactive approaches to privacy.

The technical community has more to offer. Standard setting bodies have an important role to play in enabling privacy. Identifying approaches to the development of Web and Internet standards that provide sound building blocks for privacy protective designs, defaults, and policies requires a sustained and concerted effort. Equally importantly, the call for privacy considerations to inform design should not be exclusively led or dictated by lawyers or regulators. The effort must be a partnership. Identifying approaches to build privacy in will require active engagement between computer scientists and engineers, and privacy experts from other disciplines.

Privacy, like security, should yield a set of technical properties that can be defined and realized in various parts of the ecosystem. The properties that privacy may drive at the level of Internet or Web standards may be quite thin—in fact they may be properties that promote a broad set of policies. For example, properties of transparency, the ability to associate rules to data, and user control would provide hooks for privacy as well as other values (accessibility, choice and competition, for example).

Regardless of the ultimate outcome of the web tracking activities under consideration, the W3C should continue to expand its work on privacy. The W3C is uniquely positioned to sort out the appropriate role for Web standards in facilitating privacy solutions and has institutional experience building the bridges between disparate communities that is required to do this work.

Sincerely,

Deirdre K. Mulligan