

Definitions ^{1st/3rd party}
 ^{Beta}
 behaviors
 technical actions
 narrow scope
 DNT header
 Other Internet / Web privacy problems
 Low-hanging fruit
 Study ecosystem, roles of entities
 Standardize ^{DNT} opt out = OBA
 Good enough ^{Use communication}

Incubator group
 Move quickly into wgs
 Interest group (ongoing)
 Policy forum

1 year
 Beta soon - 6 weeks

Coordination / outreach needs

- ad trade associations
 - more social networks
 response header
 Location
 User / economic research
 Landscape document

Strategy to engage
 if missing groups
 More volunteers to help bridge
 Coordination outside US

6 months

How we got here

- Founded by Tim Berners-Lee
- Based at MIT (Cambridge, MA), ERCIM (Sophia Antipolis, France), Keio University (Tokyo)
- World-wide membership of 319 organizations
- Develops standards for the Web in a vendor-neutral, open, transparent process
- <http://www.w3.org/Consortium/join>

About W3C

Call For Participation

Background

As part of the ongoing larger online privacy debate, the discussion about online tracking (for example for behavioral advertising) and [possible countermeasures](#) has picked up a lot of momentum. This discussion has been reflected in policy papers on user privacy on the Web from the United States [Federal Trade Commission](#) and [Department of Commerce](#).

Several vendors are offering measures that are intended to permit users to opt out of this tracking, or to prevent tracking by Web sites that are known to engage in these practices. For example:

- [Microsoft announced](#) the inclusion of anti-tracking technology based on tracking protection lists in IE9. This technology was [submitted](#) to W3C ([see staff comment](#)).
- [Mozilla announced](#) support for a "do not track" header.
- [Google announced](#) a browser extension that permits users to persist opt-out cookies.

Similar technology is deployed in a number of plugins for various browsers, including, for example, [NoScript](#), [AdBlock plus](#), [TACO](#), and [PrivacyChoice](#).

As a result of its 2011 strategic planning exercise, the W3C is reinforcing efforts in the Web privacy space, beyond its current involvement in the European [PrimeLife](#) project.

Goals and Scope



Hosted by the Center for
Information Technology Policy
at Princeton University

Workshop sponsors:



YAHOO!

Google

mozilla

Microsoft

Princeton, 28/29 April 2011

Google Chrome, Firefox Adding 'Do Not Track' Tools

BIG NEWS: Internet | Twitter | NASA | Cyber Security | Energy Debates | More...

LOG IN | SIGN UP

THE HUFFINGTON POST
FEBRUARY 7, 2011

FIND EXACTLY WHAT YOU'RE LOOKING FOR WITH BING.
Dorset, England

FRONT PAGE | POLITICS | BUSINESS | MEDIA | ENTERTAINMENT | COMEDY | SPORTS | STYLE | WORLD | GREEN | FOOD | TRAVEL | TECH
LIVING | HEALTH | DIVORCE | ARTS | BOOKS | RELIGION | IMPACT | EDUCATION | COLLEGE | NY | LA | CHICAGO | DENVER | BLOGS

White iPhone 4 Shelf Space Spotted
U.S. Has Secret Tools To Force Internet On Dictators
Sprint To Unveil Tablet-Like Phone?

Google Chrome, Firefox Adding 'Do Not Track' Tools
DANA WOLLMAN : 01/24/11 05:20 PM

Inspiring | Funny | Obsolete | Scary | Must-Have | Amazing | Innovative | Nerdy

Read More: [Chrome Do Not Track](#), [Firefox Do Not Track](#), [Firefox Tracking](#), [Google Chrome](#), [Google Chrome Do Not Track](#), [Google Chrome OS](#), [Technology News](#)

NEW YORK — The Firefox and Google Chrome browsers are getting tools to help users block advertisers from collecting information about them.

Fowler, a technology and privacy officer for Firefox maker Mozilla, said the "Do Not Track" tool will be the first in a series of steps designed to guarantee privacy. He didn't say when the tool will be available.

Google Chrome users can now download a browser plug-in that blocks advertisers — but only from ad networks that already let people decline personalized, targeted ads. According to Google Inc., these include the top 15 advertising networks, as rated by the research group comScore, a group

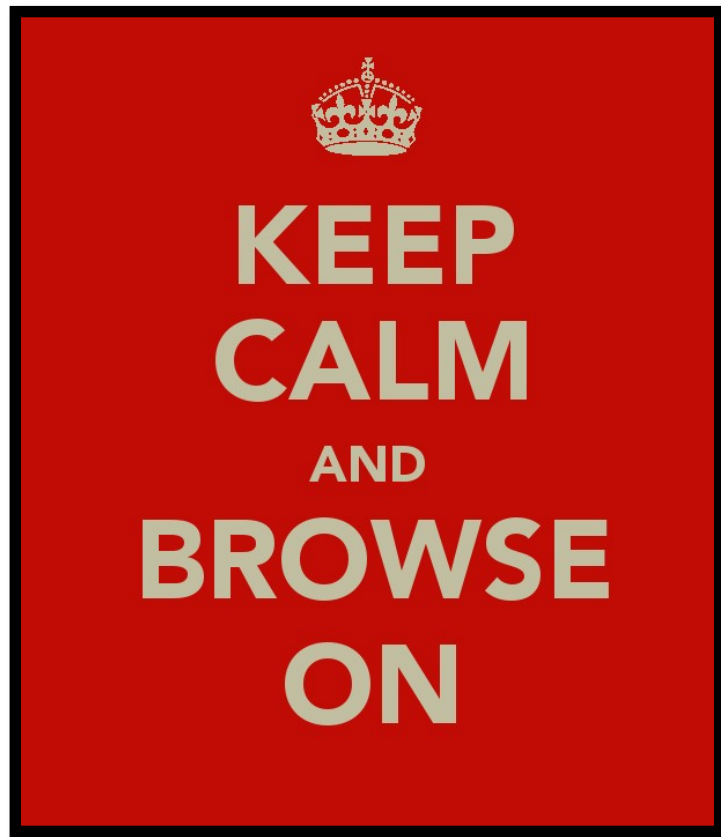
Learn the truth about "GASLAND" CLICK HERE
anga

FOLLOW HUFFINGTON POST

MOST POPULAR ON HUFFPOST 1 of 2

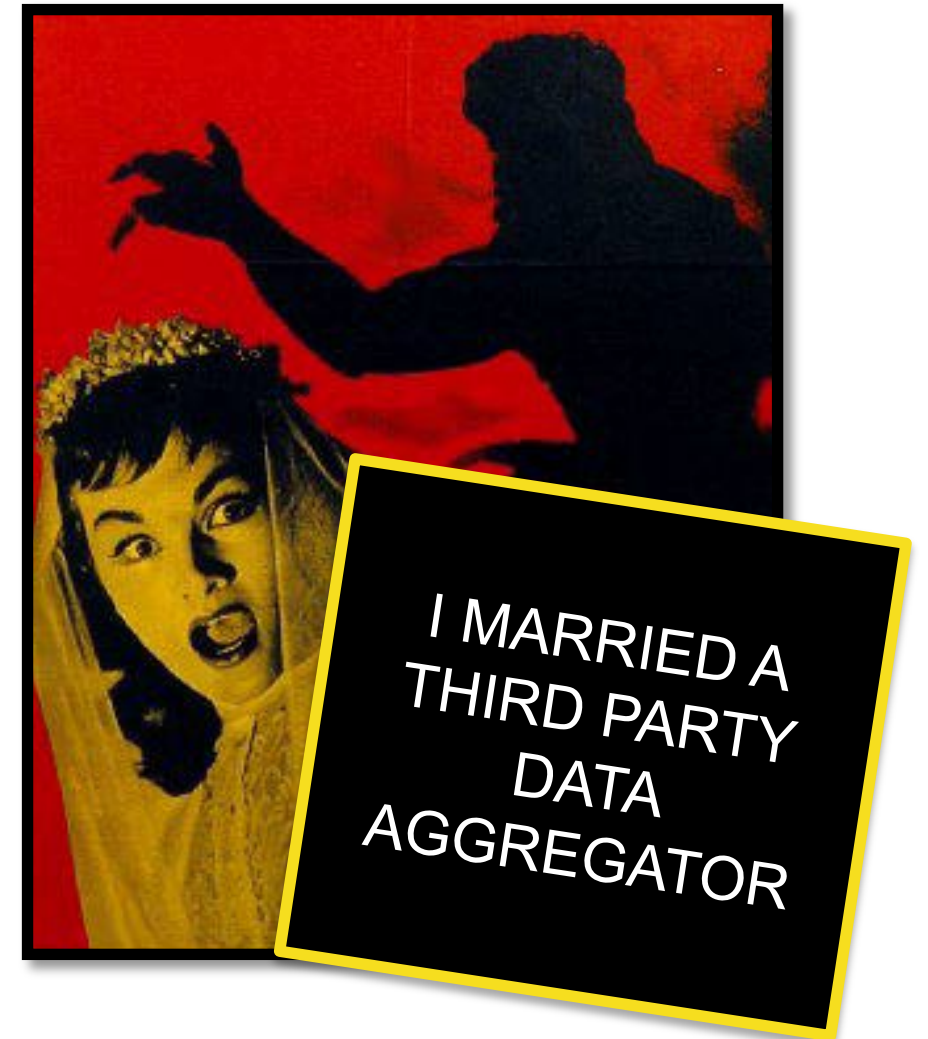
Web Tracking Is Here

What's a user supposed to think?



Everything is fine!

The internet is just like
the friendly shopkeeper
on your block.



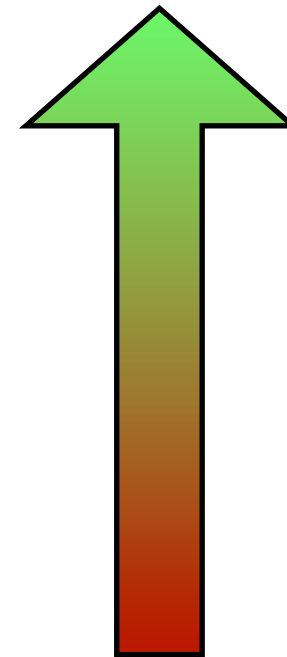
YOU ARE IN SERIOUS
DANGER.

What they know can –
and does – hurt you.

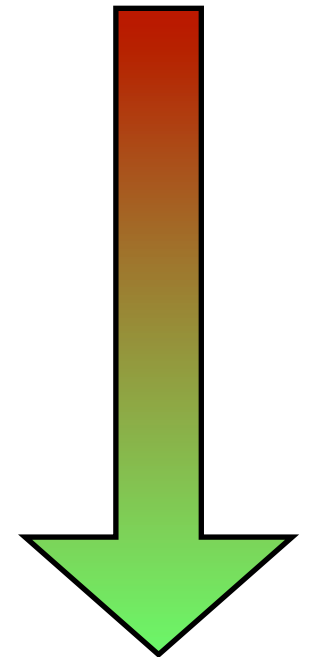
Observations

- Users do hear “Do Not Track” as related to being tracked online...
- ...and many think it means they will not be tracked at all, **including collection**
- Options to address the expectations gap:
 - Build DNT to match expectations
 - Create one definition of DNT and communicate it very clearly
 - Create one definition and communicate exceptions
 - Allow multiple definitions and communicate them in novel ways
Suggestion: HTTP header response
 - Put details into privacy policies and help files

**Ease of
Use**



**Ease of
Adoption**

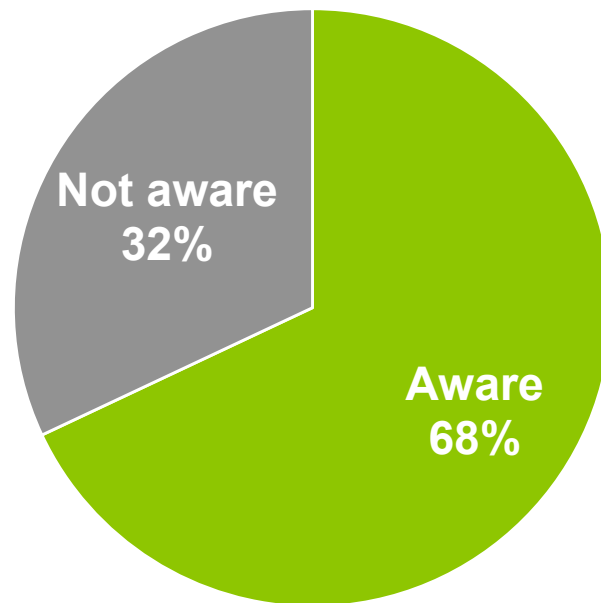


Tracking Expectations

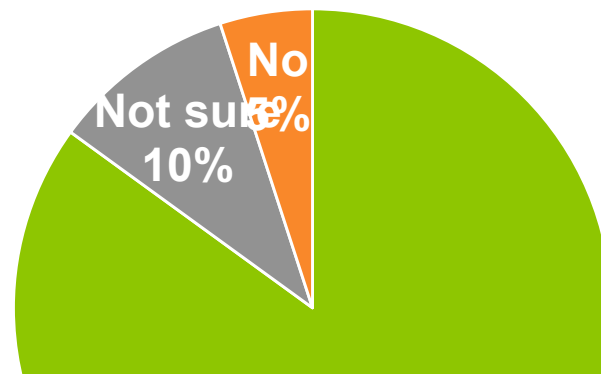
And let's not forget about mobile and Native apps



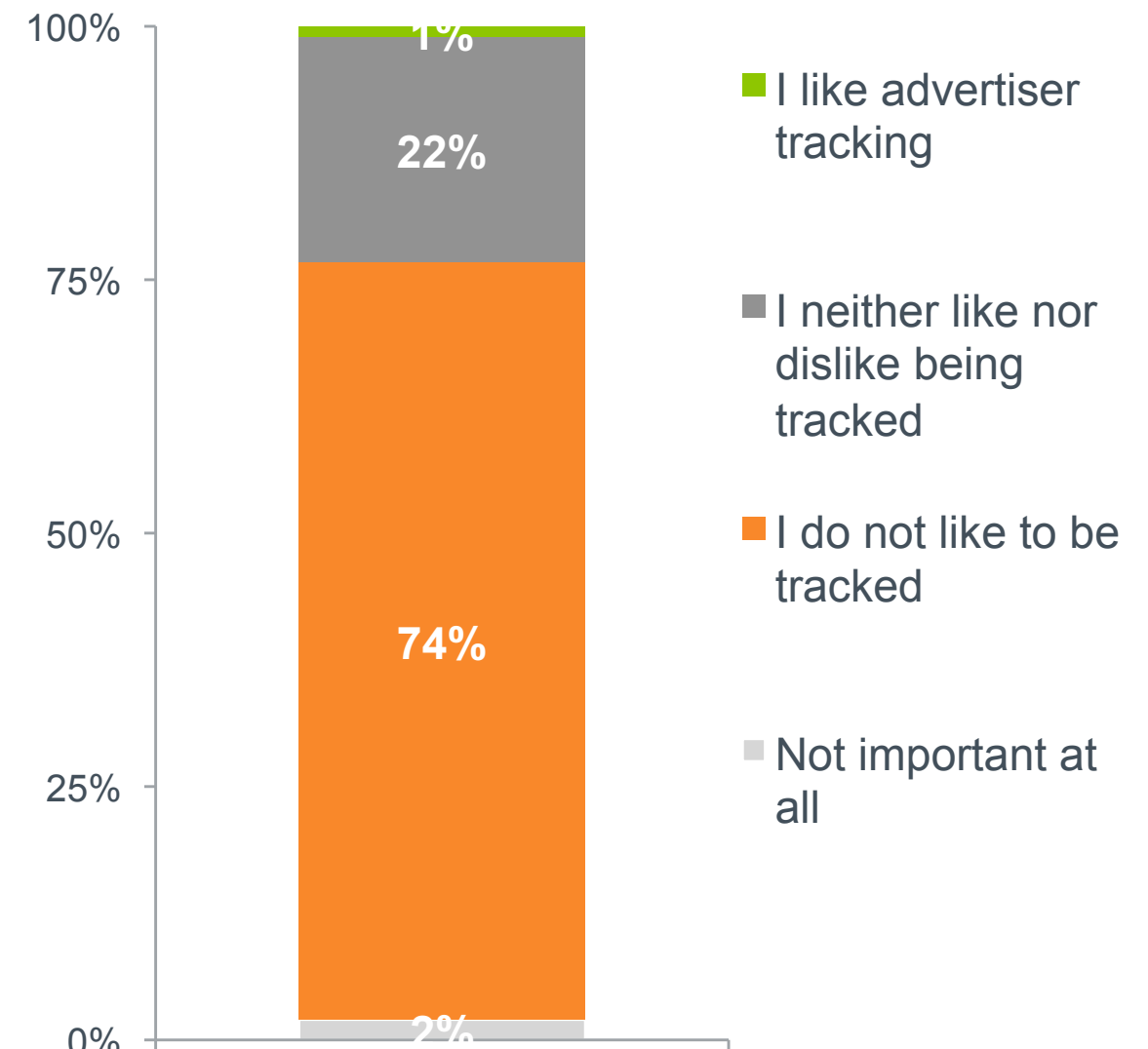
Are you aware that advertisers are tracking your mobile activities and delivering ads targeted to you based on your behavior?



Are you interested in being able to opt in or out of targeted mobile ads?



Feelings About Advertiser Tracking



Tracking Expectations



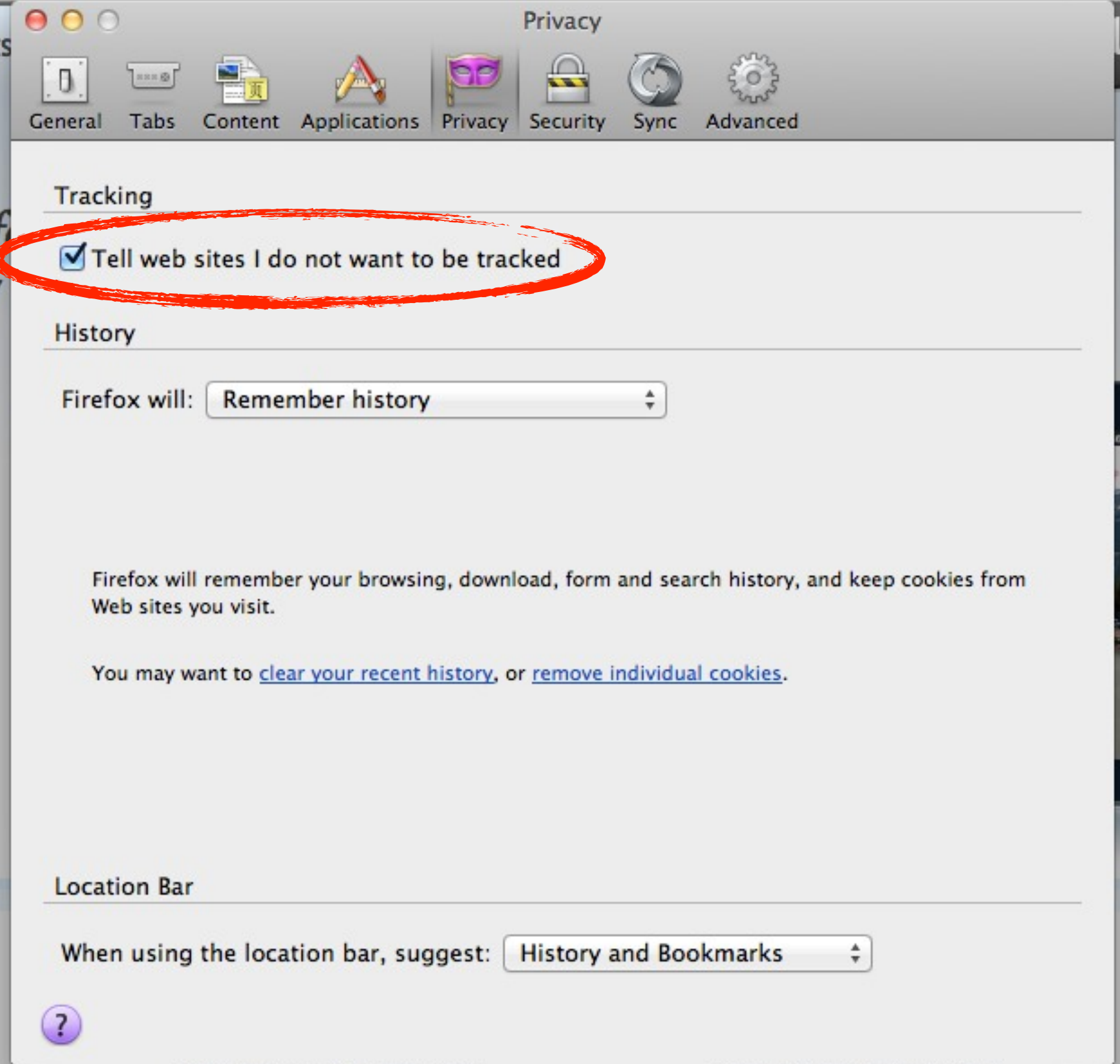
Good news! Your Firefox
NOW STAY

Get easy and safe access to your history, bookmarks, tabs and passwords on all your devices.

Get in Sync »

Get *Firefox*

If you need a fresh new copy of Firefox, you can get it here:



Mozilla: HTTP header

Apple Adds Do-Not-Track Tool t...

TECHNOLOGY | APRIL 14, 2011

Apple Adds Do-Not-Track Tool

Article

Video

Stock Quotes

Email

Print

Save

Like 206

0

By NICK WINGFIELD

Apple Inc. has added a do-not-track privacy tool to a test version of its latest Web browser for keeping customers' online activities from being monitored by Google Inc.

Introducing Safari 5.

It has innovative new features that improve the way you use the web. And powerful new tools to help developers enhance and customize the browsing experience altogether. [Learn more](#)

Safari 5

Free download

For Mac + PC

Apple has added a do-not-track privacy tool to a test version of its latest Web browser for keeping customers' online activities from being monitored - leaving Google as the only major company with a web browser that hasn't taken this step.

The tool is available only to developers. The final version of the operating system is scheduled to be released to the public this summer. Mentions of the do-not-track feature in Apple's Safari browser began to appear recently in online discussion forums and on Twitter

The move by the Cupertino, Calif., company leaves Google Inc. as the only major browser provider that hasn't yet committed to

Develop

Open Page With User Agent

Show Web Inspector

Show Error Console

Show Snippet Editor

Show Extension Builder

Start Debugging JavaScript

Start Profiling JavaScript

✓ Send Do Not Track HTTP Header

Enable WebGL

Disable Caches

Disable Images

Disable Styles

Disable JavaScript

Disable Runaway JavaScript Timer

Disable Site-specific Hacks

com

Reader

Google

MO

Click here to find out more

We will not rest  UB

Available to WSJ.com Subscribers

Apple: "Develop"

Safari 5.1

Tracking Protection Lists

Below are several Tracking Protection Lists (also called TPLs) created by companies and organizations that want to help consumers understand and make choices about their online privacy. You can add individual lists by clicking the "Add TPL" links on the right side of the page. To manage your lists, click on the **Tools** button, point to **Safety**, then click **Tracking Protection**. These tracking protection lists were created by their respective authors, who are solely responsible for maintaining the lists and for their content. Microsoft does not control any of these lists. [Click here for answers to commonly asked questions about TPLs.](#)



Abine, The Online Privacy Company, is the leading provider of online privacy solutions for consumers. Abine's products and services allow regular people to regain control over their personal information while continuing to browse, interact, and shop online.

[Add TPL](#)

Abine's Tracking Protection List blocks many online advertising and marketing technologies that can track and profile you as you browse the Web. This list is updated weekly to keep you safer and more private.

[Visit the Abine website for more information about this Tracking Protection List.](#)



EasyPrivacy Tracking Protection List is based on the popular EasyPrivacy subscription for Adblock Plus and is managed by the well-known EasyList project, which serves nearly ten million daily users and has a large support forum with dozens of experienced members able to assist resolving any issues that may arise.

[Add TPL](#)

[Visit the EasyList website for more information about this Tracking Protection List.](#)

MS: Tracking Protection Lists

Web Tracking Protection

W3C Member Submission 24 February 2011

This version:

<http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224/>

Latest version:

<http://www.w3.org/Submission/web-tracking-protection/>

Editors:

Andy Zeigler, Microsoft Corporation
Adrian Bateman, Microsoft Corporation
Eliot Graff, Microsoft Corporation

Copyright© 2011 Microsoft Corporation

This document is available under the [W3C Document License](#). See the [W3C Intellectual Rights Notice and Legal Disclaimers](#) for additional information.

Abstract

The Web Tracking Protection specification is designed to enable users to opt-out of online tracking. The platform has two parts:

- Filter lists, which can enforce user privacy preferences by preventing the user agent from making unwanted requests to web servers that track users.
- A user preference, which is an HTTP header and a DOM property, to be used by web servers to respect the user's privacy.

Together these technologies can be used to enforce privacy protection for users, and provide access to content and services that respect user privacy preferences.

MS: Member Submission

Server Side Responses

Publishers/Sites

- Select ad networks that honor DNT header
- Optionally reduce on-site tracking with presence of header
- Update privacy messaging and privacy policies
- Consider other server-side innovations / responses

Ad/Data Companies

- Treat presence of header like opt-out cookie
- Leverage respect for privacy as advantage to publishers
- Further demonstrate commitment to self-regulation and user choice and control by integrating with enhanced notification program



Service providers.



Scope of Do Not Track

MeMe Jacobs Rasmussen – VP, Chief Privacy Officer



What does it mean?

WHAT DOES TRACKING MEAN?

Fundamentally, this is a policy problem

- Informed by an analysis of technology, a constantly moving target

Multiple requirements

- Privacy rights and expectations of internet users
 - Balanced by property/security requirements of website operators.
- Jurisdiction issues
- Security/Fraud controls are needed to protect privacy online

User Expectations Vary

- Capturing intent/belief, especially implicit expectations, is hard

Security and Fraud Controls

Don't let weasel words eat away privacy protection!

Behavioral Targeting

must be:

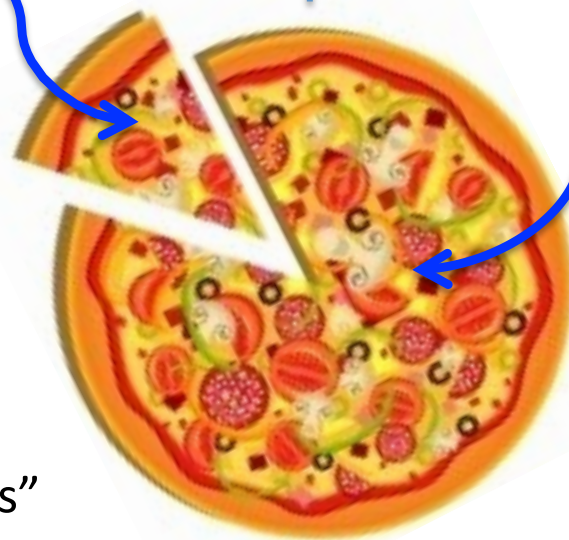
“**Web** viewing behaviors”

“from a **particular** computer”

“across **non-Affiliate** Web sites”

PII is “information about a **specific** individual...”

Sensitive Consumer Information is
“**Precise** Information...about health or medical conditions...”



Ad Delivery & Reporting + other uses not covered

“Ad Delivery is the delivery of online advertisements...” basically almost everything else not “covered by the definition of Online Behavioral Advertising.”

What about non-OBA tracking?

Scope limitations

Desired Properties of Tracking Controls

- **Simple**
- **Universal**
- **Comprehensive**
- **Inclusive**
- **Effective**
- **Seamless**
- **Persistent**
- **Interoperable**



Requirements



As currently conceived, DNT
does not facilitate a transparent,
two-way dialog
Between the **Consumer**
and the **Publisher**

Business Interests

The Goal of Do-Not-Track should be to Provide Meaningful Choices

The Do-Not-Track header succeeds because it:

- is a communication tool rather than a technical blocking solution
- balances the interests of consumers and the needs of businesses
- is technically simple
- enables technologies to respond in a manner that maintains the desired consumer experience
- will encourage marketplace innovation in consumer choice



Business Interests



Regulatory Concerns



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

A few subtle statements...

Andrew Patrick, Ph.D.
IT Research Analyst

across jurisdictions

web trackers are breaking the law*

*** third parties, Canadian law**

Consumer Criteria for DNT

1. Universal: single opt-out covers all would-be trackers
2. Usable: easy to find, understand, and use
3. Persistent: opt-out doesn't vanish
4. Effective and enforceable: covers all tracking technologies
5. Collection: controls collection*, not just some uses (e.g. ads)

FTC criteria for do not track

breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which

measures of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).';

5) Article 5(3) shall be replaced by the following:

'3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.';

6) Article 6(3) shall be replaced by the following:

'3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or

Article 5(3)

Do Not Track: The Regulators' Challenge.

The fine people at the UC Berkeley law school have pulled together an [amazing two-day workshop about Web Tracking in Brussels](#). The conversation kicked off today with European Commissioner Neelie Kroes [talking about privacy, self-regulation and do not track](#), and with Director General Robert Madelin and FTC Commissioner Julie Brill on the subsequent panel. Together, the three handed a sizable challenge to the Web standards community: Standardize Do Not Track within a year (or less), be transparent, be inclusive.

[Neelie Kroes'](#) key points: While the advertising industry's self-regulatory efforts are important and welcome, they aren't enough. Tracking protection cannot be limited to just cookies (and cannot ignore other ways to create client state); it cannot be limited to just advertising or other specific sectors; and it cannot be limited to just the use of the data; instead, tracking protection needs to apply to data collection as well. Also, industry needs to address both Web and mobile tracking, and soon. [Kroes' challenge to industry](#): Standardize Do Not Track by June 2012. Come to the standards table.

FTC Commissioner Julie Brill spoke about the FTC's efforts in the space over the last several years. She reminded us of the FTC's [staff paper](#) and the [five principles for an effective Do Not Track technology](#): 1. It must be easy to use (in fact, asked Brill, wouldn't it be nice if the advertising industry was making opt-outs as easy to use as ads); 2. It must be effective; 3. It must be universal; 4. It must deal with collection as well as with use of information; 5. It must be persistent (and not go away after 5 days, or when you delete your cookies). As a significant footnote, Brill pointed out the special sensitivity of geolocation information, and the need for minimization there.

On standardization, Brill's worry is that industry standardization might be too slow a process, and could possibly take beyond mid 2012.

Finally, [Robert Madelin](#) (Director General for the European Commission DG Information Society and Media) put the tracking conversation into the context of Internet regulation overall ("it can't be a random walk between individual jurisdictions") and the eG8, and into broader thinking about effective self-regulatory approaches. The sweet spot, according to Madelin, is somewhere in the middle between strongly mandated co-regulation and purely industry-led self-regulation: industry-led, yes – but inclusive, with a clear process, and with clear accountability and transparency to the public, and with a preference for shipping over the sort of perfection that can hold up agreement forever.

June 16/17, Brussels

Tracking Protection Working Group Charter

This document is under formal W3C Advisory Committee review.

For informal discussion of the proposal, send comments and subscribe to public-privacy@w3.org ([public archives](#)).

The **mission** of the Tracking Protection Working Group, part of the [Privacy Activity](#), is to improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements.

Join the Tracking Protection Working Group.

End date	31 July 2012
Confidentiality	Proceedings are public
Initial Chairs	Co-Chairs: To Be Announced
Initial Team Contact	Nick Doty, W3C/MIT (FTE %: 25)
Usual Meeting Schedule	Teleconferences: Weekly Face-to-face: 3-4 per year

1. Scope

The Working Group will produce Recommendation-track specifications for a simple machine-readable preference expression mechanism ("Do Not Track") and technologies for selectively allowing or blocking tracking elements.

Proposed technologies for the user preference that the Working Group will consider include, but are not limited to, the use of an HTTP header to signal the preference and a site's response, and the use of a ECMAScript API or DOM property for the same purpose. For selective blocking of tracking elements, the Working Group will consider, but is not limited to, black and white listing, as proposed in the [Web Tracking Protection submission](#).

Additionally, the Working Group will define the scope of the user preference and practices for compliance with it in a way that will inform and be informed by the technical specification. The group will actively engage governmental, industry, academic and advocacy organizations to seek global consensus definitions and codes of conduct.

The Working Group may investigate monitoring of implementation and conformance to Recommendations by both user agents and Web sites.

Approved, kicking off

- **Tracking Preference Expression (Do Not Track), Recommendation.**

This specification defines the technical mechanisms for expressing a Do Not Track preference, for example as an HTTP header or a DOM property. It may include mechanisms for sites to signal whether and how they honor this preference.

- **Tracking Preference Expression Definitions and Compliance, Recommendation.**

This specification defines the meaning of a Do Not Track preference and sets out practices for Web sites to comply with this preference.

- **Tracking Selection Lists, Recommendation.**

This specification defines a format for interchangeable lists for blocking or allowing Web tracking elements and expected user agent interpretation of this format.

Deliverables



9/21-22, Cambridge, MA, US

<http://www.flickr.com/photos/seeminglee/3791607622/sizes/l/in/photostream/>