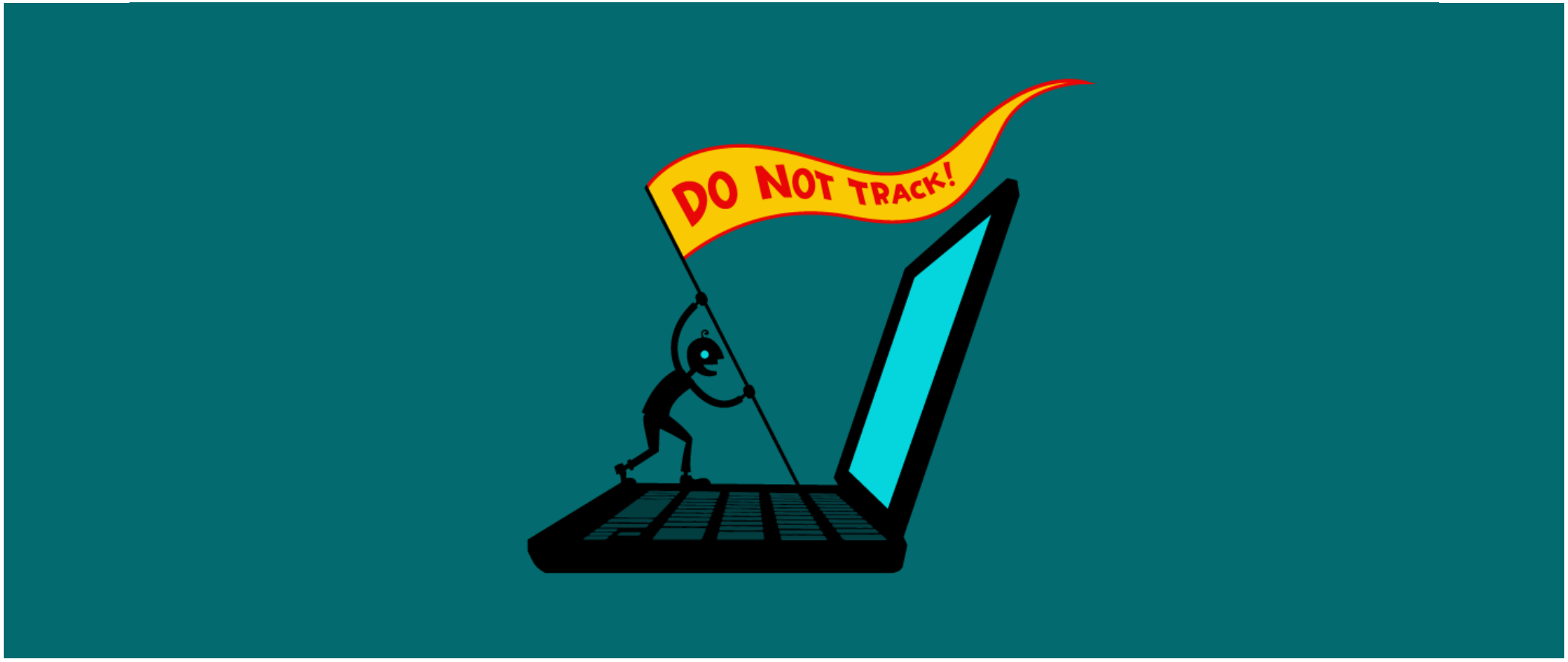
Do Not Track



Do Not Track (DNT) is a way to keep users' online behavior from being followed across the Internet by behavioral advertisers, analytics companies, and social media sites. It combines both technology (a way to let users signal whether they want to be tracked) as well as a policy framework for how companies should respond to that signal.

Tracking Users: From Cookies to Device Fingerprinting

Online tracking began in the late 1990s but has expanded massively in the last decade. Advertising is the main business model financing media production on the open web, and the drive to increase revenue by targeting ads to selected users has led to the creation of a plethora of companies dedicated to monitoring our clicks, searches, and reading habits as we move around the Internet. While technologists have long worried about the privacy implications, it was the Wall Street Journal's What They Know series in 2010 that brought widespread public attention to the issue by showcasing how marketers gather data on online users.

Much of this tracking happens via cookies. The HTTP cookie, invented at Netscape in 1994, came into life as an innocent and essential tool for the web; cookies make possible "stateful" user interfaces such as user accounts and logins, multi-page

forms, or online shopping carts. But cookies also allow sites to store a unique ID in your browser, and therefore to track you—and if a company is present on multiple websites, it can track your visits to each of those sites. In other words, a company can use cookies to construct a detailed overview of users' activity. Many people feel this is an invasion of their privacy, and want to be able to block, limit or delete their cookies.

Unfortunately, more recent technologies have fostered the development of cookie-like tracking systems that are harder for a user to detect or delete, and can provide marketers with a rich source of data about an individual. Today, online tracking companies use supercookies and fingerprints to follow people who try to delete their cookies, and the leakage of user IDs from social networks and similar sites has often given them an easy way to identify the people they were tracking. In December 2015 EFF launched an updated version of its Panopticlick site which enables users to check their browser's resistance to different tracking techniques.

Towards a Universal Opt-out for Users: Do Not Track

Previous attempts to build user-privacy mechanisms against data collection and tracking have either failed (P3P) or are too complex and piecemeal for widespread

user-adoption. This is especially true of the ad industry's own opt-out program, AdChoices. Under this scheme ads are not targeted to users, but the underlying data collection about their activity continues. Furthermore a user's AdChoices opt-out preference is stored in a cookie, and is thus erased any time a user clears the cookies in their browser. DNT, on the other hand, was created to function as a simple, universal, and persistent opt-out from tracking. It provides users with a voice--so they can tell companies whether or not they want to be tracked online.

Here's how it works: Every time your computer sends or receives information over the Web, the request begins with some short pieces of information called headers. These headers include information like what browser you're using, what language your computer is set to, and other technical details. The Do Not Track signal is a machine-readable header indicating that you don't want to be tracked. Because this signal is a header, and not a cookie, users can clear their cookies at will without disrupting the functionality of the Do Not Track flag.

DNT at the W3C

The idea of sending Do Not Track messages in HTTP headers was first suggested in 2009, although the history of the term is older and was once associated with other

approaches. The proposal was endorsed by the US Federal Trade Commission the following year and floated as an alternative to regulation. In 2011 Safari and Firefox implemented support for the signal as a user-configured preference in the browser, but websites did not alter their behaviour in response to it. Around the same time, Internet Explorer shipped with an anti-tracking feature built-in which actually blocked trackers and ads.

Excitement about DNT led to creation of a working group at the World Wide Web Consortium (W3C) in September 2011. The W3C's task was to standardise the technical interaction between browsers and servers, and to tease out an agreement on the policy websites should apply on receipt of the signal.

The working group included publishers, advertising companies, browser and software companies and user advocates including EFF. There was hope of a grand compromise amongst rival interests, but after some early progress the working group stalled in 2012. The following year the main trade organisation of the online advertising industry, the Digital Advertising Alliance (DAA), pulled out and it became clear that a big tent solution was not going to be possible. In the meantime the scale of tracking continued to increase: a 2016 survey of the top one million

websites found that top sites hosted between 25 and 30 third parties, many of them trackers.

EFF's DNT Policy and Privacy Badger

Faced with the failure of the W3C process, EFF devised a two-pronged strategy that would provide immediate self-defense for users against tracking, while simultaneously giving advertisers an incentive to stop non-consensual tracking.

First, EFF began work on a DNT policy of its own, based on stronger privacy criteria than would have been possible at the W3C. EFF's DNT policy requires that users who have turned on the DNT signal are not tracked without their clear and informed consent. Otherwise, it has strict limitations on what data can be collected and how long that data can be retained. (It also includes exceptions that respect the ordinary functionality of a site, that allow measures for security purposes and prevent fraud, and allow data analysis techniques that protect the anonymity of the users.) The policy was launched in August 2015 together with a coalition including software companies Disconnect and Adblock, analytics provider Mixpanel, the publisher Medium.com and search engine DuckDuckGo. In autumn 2015 Adzerk became the first advertising company to announce support for the policy.

And what if a website doesn't commit to honoring EFF's DNT policy? That's where the second prong of EFF's strategy comes in: a browser extension for Firefox and Chrome, called Privacy Badger, which blocks tracking and enforces DNT even in the absence of voluntary industry compliance.

Privacy Badger works by watching for third party calls on websites, checking if they are present over multiple sites, and blocking them if they appear to be related to tracking. To the user, the most visible result is that ads end up being blocked, because most ads have a tracking component built in to them.

Despite this, Privacy Badger is not an adblocker, but rather a tracker blocker, intended to incentivize ad-tech companies to develop privacy-friendly forms of advertising. Whereas adblockers punish all publishers indiscriminately, Privacy Badger offers good actors the option of having their content (including ads) unblocked if they adopt EFF's DNT policy.

In other words, the Privacy Badger/DNT Policy mechanism offers publishers, advertisers and third parties access to a universe of users from which they are otherwise excluded, if they play fair, thus giving them an incentive to change their ways. EFF's goal is to persuade other content blockers to also block based on

whether or not a website follows EFF's DNT policy and reward companies who commit to respecting users' privacy preferences.

Current Developments

Of course the story of Do Not Track hasn't ended yet. In August 2015 the W3C published two proposed standards, the Tracking Preference Expression (TPE) and Tracking Compliance and Scope (TCS). The TPE defines the technical specification for DNT, which is useful and which EFF supports. But we oppose the TCS, the policy document setting out what it means to comply with DNT, because it contains loopholes which could be exploited by unscrupulous actors to continue wholesale tracking while purporting to support DNT. This is not acceptable: users deserve a meaningful DNT standard that provides them with clear guarantees.

At the same time, while the prospects of federal regulation in the US have receded somewhat, the European Union passed a General Data Protection Regulation envisaging applications of the DNT mechanism.

These events are unfolding in the context of seismic shifts in power online. Firstly the open web, where publishers and readers encounter one another freely, is being

squeezed by closed platforms - e.g. mobile apps, Facebook - which have become the dominant route to journalism. Advertising income which once went to publishers is now siphoned off by the platforms and adtech intermediaries. Secondly ads have increased both in volume and intrusiveness, propelling the rise of adblocking. Worse still, by allowing third party tracking, publishers have surrendered control over their websites and the exclusivity of the relationship with their readers, The result is a loss of both trust and ultimately income (users can always be targeted more cheaply elsewhere) and the exposure of users' reading habits and browsing history. This environment can deliver neither sustainable independence for content producers nor privacy for users – there must be a better way.

Respectful Advertising

This brings us to the fundamental challenge: the publishing and advertising ecosystem must reform in order to recover the user trust lost due to widespread bad practices in the industry. Faced with the mass adoption of adblockers, the industry has had to respond to demand for forms of 'acceptable' advertising, which does not abuse the user's attention with obnoxious pop-ups or annoying audio. In the same way, advertisers must also commit to respectful advertising: advertising that doesn't come at the cost of users' privacy and doesn't track their movements across the web. Our DNT work is a call for such an approach, one which gives users control,

puts their privacy first, and enables useful ads that will in turn sustain the web we know and love.

Archived version of [*Do Not Track – Universal Web Tracking Opt Out*]

We're in the Uncanny Valley of Targeted Advertising

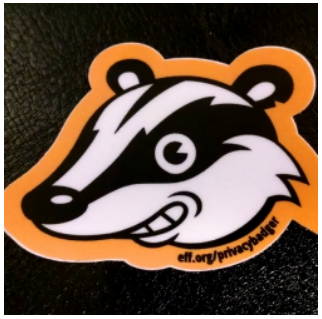
DEEPLINKS BLOG BY JASON KELLEY | APRIL 20, 2018

Mark Zuckerberg, Facebook's founder and CEO, thinks people want targeted advertising. The "overwhelming feedback," he said multiple times during his congressional testimony, was that people want to see "good and relevant" ads. Why then are so many Facebook users, including leaders of state in the U.S. Senate...

DEEPLINKS BLOG BY ANDRÉS ARRIETA | APRIL 10, 2018

A New Welcome to Privacy Badger and How We Got Here

The latest update to Privacy Badger brings a new onboarding process and other improvements. The new onboarding process will make Privacy Badger easier to use and understand. These latest changes are just some of the many improvements EFF has made to the project, with more to come! ...



DEEPLINKS BLOG BY ANDRÉS ARRIETA | MARCH 26, 2018

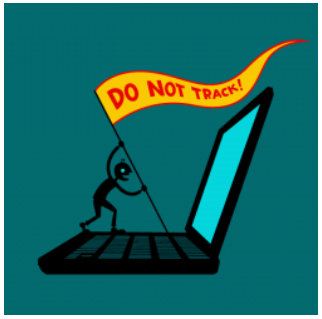
One Response to the Cambridge Analytica Scandal: Block Facebook's Tracking With Privacy Badger

With Facebook in a dominant position in hosting a huge portion of the world's social conversation, we've been worried about the incredible power the company has accumulated and the risks that poses to privacy and democratic conversation. Last week's news about Facebook and Cambridge Analytica has shown that our worst...

DEEPLINKS BLOG BY ALAN TONER, ANDRÉS ARRIETA | NOVEMBER 1, 2017

Do Not Track Implementation Guide Launched

Today we are releasing the implementation guide for EFF's Do Not Track (DNT) policy. For years users have been able to set a Do Not Track signal in their browser, but there has been little guidance for websites as to how to honor that request. EFF's DNT policy...



DEEPLINKS BLOG BY ALAN TONER | AUGUST 28, 2017

Twitter (and Others) Double Down on Advertising and Tracking

In June, Twitter discontinued its support for Do Not Track (DNT), the privacy-protective browser signal it has honored since 2012. EFF argued that Twitter should reconsider this decision, but that call has gone unheeded. In response, EFF's Privacy Badger has new features to mitigate user tracking both...

ELECTRONIC FRONTIER FOUNDATION

The leading nonprofit defending digital privacy, free speech, and innovation.

FOLLOW EFF:

CONTACT

- General
- Legal
- Security
- Membership
- Press

ABOUT

- Calendar
- Volunteer
- Victories
- History
- Internships
- Jobs
- Staff

ISSUES

- Free Speech
- Privacy
- Creativity & Innovation
- Transparency
- International
- Security

UPDATES

- Blog
- Events
- Press Releases
- Whitepapers

PRESS

- Press Contact
- Press Materials

DONATE

- Join or Renew Membership Online
- One-Time Donation Online
- Shop
- Other Ways to Give