A privacy-friendly Do Not Track (DNT) Policy

This page provides a copy of EFF's DNT Policy, a text file that domains can post in verbatim form to unilaterally commit to respecting a meaningful version of Do Not Track, in such a way that other software can tell they have done so. A human readable summary is available, and there are frequently asked questions below.

```
Do Not Track Compliance Policy

Version 1.0

This domain complies with user opt-outs from tracking via the "Do Not Track"
or "DNT" header  [http://www.w3.org/TR/tracking-dnt/].  This file will always
be posted via HTTPS at https://example-domain.com/.well-known/dnt-policy.txt
to indicate this fact.

SCOPE

This policy document allows an operator of a Fully Qualified Domain Name
("domain") to declare that it respects Do Not Track as a meaningful privacy
opt-out of tracking, so that privacy-protecting software can better determine
whether to block or anonymize communications with this domain.  This policy is
intended first and foremost to be posted on domains that publish ads, widgets,
images, scripts and other third-party embedded hypertext (for instance on
widgets.example.com), but it can be posted on any domain, including those users
visit directly (such as www.example.com). The policy may be applied to some
domains used by a company, site, or service, and not to others.  Do Not Track
may be sent by any client that uses the HTTP protocol, including websites,
mobile apps, and smart devices like TVs. Do Not Track also works with all
protocols able to read HTTP headers, including SPDY.

NOTE: This policy contains both Requirements and Exceptions. Where possible
terms are defined in the text, but a few additional definitions are included
at the end.

REQUIREMENTS
```

```
When this domain receives Web requests from a user who enables DNT by active
ly
choosing an opt-out setting in their browser or by installing software that
is
primarily designed to protect privacy ("DNT User"), we will take the followi
ng
measures with respect to those users' data, subject to the Exceptions, also
listed below:

1. END USER IDENTIFIERS:

  a. If a DNT User has logged in to our service, all user identifiers, such
as
     unique or nearly unique cookies, "supercookies" and fingerprints are
     discarded as soon as the HTTP(S) response is issued.



     Data structures which associate user identifiers with accounts may be
     employed to recognize logged in users per Exception 4 below, but may no
t
     be associated with records of the user's activities unless otherwise
     excepted.

  b. If a DNT User is not logged in to our service, we will take steps to en
sure
     that no user identifiers are transmitted to us at all.

2. LOG RETENTION:

  a. Logs with DNT Users' identifiers removed (but including IP addresses an
d
     User Agent strings) may be retained for a period of 10 days or less,
     unless an Exception (below) applies. This period of time balances priva
cy
     concerns with the need to ensure that log processing systems have time
to
     operate; that operations engineers have time to monitor and fix technic
al
     and performance problems; and that security and data aggregation system
s
     have time to operate.

  b. These logs will not be used for any other purposes.
```

```
3. OTHER DOMAINS:

  a. If this domain transfers identifiable user data about DNT Users to
     contractors, affiliates or other parties, or embeds from or posts data to
     other domains, we will either:

  b. ensure that the operators of those domains abide by this policy overall
     by posting it at /.well-known/dnt-policy.txt via HTTPS on the domains in
     question,

    OR

     ensure that the recipient's policies and practices require the recipient
     to respect the policy for our DNT Users' data.

    OR

     obtain a contractual commitment from the recipient to respect this policy
     for our DNT Users' data.

    NOTE: if an “Other Domain” does not receive identifiable user information
    from the domain because such information has been removed, because the
    Other Domain does not log that information, or for some other reason, these
    requirements do not apply.

  c. "Identifiable" means any records which are not Anonymized or otherwise
     covered by the Exceptions below.

4. PERIODIC REASSERTION OF COMPLIANCE:

  At least once every 12 months, we will take reasonable steps commensurate
  with the size of our organization and the nature of our service to confirm
  our ongoing compliance with this document, and we will publicly reassert our
  compliance.

5. USER NOTIFICATION:
  a. If we are required by law to retain or disclose user identifiers, we wi
ll
     attempt to provide the users with notice (unless we are prohibited or i
t
     would be futile) that a request for their information has been made in
     order to give the users an opportunity to object to the retention or
     disclosure.

  b. We will attempt to provide this notice by email, if the users have give
n
     us an email address, and by postal mail if the users have provided a
     postal address.

  c. If the users do not challenge the disclosure request, we may be legally
     required to turn over their information.

  d. We may delay notice if we, in good faith, believe that an emergency
     involving danger of death or serious physical injury to any person
     requires disclosure without delay of information relating to the
     emergency.

EXCEPTIONS

Data from DNT Users collected by this domain may be logged or retained only
in
the following specific situations:

1. CONSENT / "OPT BACK IN"

  a. DNT Users are opting out from tracking across the Web.  It is possible
     that for some feature or functionality, we will need to ask a DNT User
to
     "opt back in" to be tracked by us across the entire Web.



  b. If we do that, we will take reasonable steps to verify that the users w
ho
     select this option have genuinely intended to opt back in to tracking.
     One way to do this is by performing scientifically reasonable user
     studies with a representative sample of our users, but smaller
     organizations can satisfy this requirement by other means.

  c. Where we believe that we have opt back in consent, our server will
```

```
     send a tracking value status header "Tk: C" as described in section 6.2
     of the W3C Tracking Preference Expression draft:

     http://www.w3.org/TR/tracking-dnt/#tracking-status-value

2. TRANSACTIONS

   If a DNT User actively and knowingly enters a transaction with our
   services (for instance, clicking on a clearly-labeled advertisement,
   posting content to a widget, or purchasing an item), we will retain
   necessary data for as long as required to perform the transaction. This
   may for example include keeping auditing information for clicks on
   advertising links; keeping a copy of posted content and the name of the
   posting user; keeping server-side session IDs to recognize logged in
   users; or keeping a copy of the physical address to which a purchased
   item will be shipped.  By their nature, some transactions will require da
ta
   to be retained indefinitely.

3. TECHNICAL AND SECURITY LOGGING:

  a. If, during the processing of the initial request (for unique identifier
s)
     or during the subsequent 10 days (for IP addresses and User Agent strin
gs),
     we obtain specific information that causes our employees or systems to
     believe that a request is, or is likely to be, part of a security attac
k,
     spam submission, or fraudulent transaction, then logs of those requests

     are not subject to this policy.

  b. If we encounter technical problems with our site, then, in rare
     circumstances, we may retain logs for longer than 10 days, if that is
     necessary to diagnose and fix those problems, but this practice will no
t be
     routinized and we will strive to delete such logs as soon as possible.


4. AGGREGATION:

  a. We may retain and share anonymized datasets, such as aggregate records
of
     readership patterns; statistical models of user behavior; graphs of sys
```

```
tem
     variables; data structures to count active users on monthly or yearly
     bases; database tables mapping authentication cookies to logged in
     accounts; non-unique data structures constructed within browsers for ta
sks
     such as ad frequency capping or conversion tracking; or logs with trunc
ated
     and/or encrypted IP addresses and simplified User Agent strings.

  b. "Anonymized" means we have conducted risk mitigation to ensure
     that the dataset, plus any additional information that is in our
     possession or likely to be available to us, does not allow the
     reconstruction of reading habits, online or offline activity of groups
of
     fewer than 5000 individuals or devices.

  c. If we generate anonymized datasets under this exception we will publicl
y
     document our anonymization methods in sufficient detail to allow outsid
e
     experts to evaluate the effectiveness of those methods.

5. ERRORS:

From time to time, there may be errors by which user data is temporarily
logged or retained in violation of this policy.  If such errors are
inadvertent, rare, and made in good faith, they do not constitute a breach
of this policy.  We will delete such data as soon as practicable after we
become aware of any error and take steps to ensure that it is deleted by any
third-party who may have had access to the data.

ADDITIONAL DEFINITIONS

"Fully Qualified Domain Name" means a domain name that addresses a computer
connected to the Internet.  For instance, example1.com; www.example1.com;
ads.example1.com; and widgets.example2.com are all distinct FQDNs.

"Supercookie" means any technology other than an HTTP Cookie which can be us
ed
by a server to associate identifiers with the clients that visit it.  Exampl
es
of supercookies include Flash LSO cookies, DOM storage, HTML5 storage, or
tricks to store information in caches or etags.
```

```
"Risk mitigation" means an engineering process that evaluates the possibilit
y
and likelihood of various adverse outcomes, considers the available methods
of
making those adverse outcomes less likely, and deploys sufficient mitigation
s
to bring the probability and harm from adverse outcomes below an acceptable
threshold.

"Reading habits" includes amongst other things lists of visited DNS names, i
f
those domains pertain to specific topics or activities, but records of visit
ed
DNS names are not reading habits if those domain names serve content of a ve
ry
diverse and general nature, thereby revealing minimal information about the
opinions, interests or activities of the user.
```

Frequently Asked Questions

Why would a domain post this policy?

A domain operator may choose to post this policy because it wants to meet best-practices privacy standards, and comply with user opt-outs from tracking. It may also comply because it wants to signal to privacy protection software (like Privacy Badger, Disconnect, or AdBlock) that it respects Do Not Track, so that its third-party embeds are less likely to be blocked.

In the former case a site may post the policy on most or all of the subdomains that it operates; in the latter case it is more likely to be posted on domains intended for third-party embedding only.

Which versions of the policy are acceptable to post?

At launch time, four versions work: the preliminary, discussion drafts 0.1 and 0.2, and version 1.0. Support for the preliminary version will be phased out in the near future.

How do I comment on the discussion draft? How do I follow changes to it?

You can send comments or suggestions to dnt-policy@eff.org. There is a mailing list for announcements of major revisions to the policy here. There is also a copy of the policy on Github that you can use for pull request or issues. But be aware that Github is not (currently) compliant with this DNT policy!

I'm an advertising/tracking company and my business practices require me to set unique cookies or fingerprint everyone, even if they have the DNT flag set. Is this policy for me?

No. This policy is not intended to be compatible with businesses practices that involve the non-consensual collection of Internet users' reading habits or online activities. It is a document intended to give users strong privacy protections, which means that in the current Web environment only some companies are going to be willing and able to post it.

What does the dnt-policy.txt promise mean?

Posting the dnt-policy.txt file makes a promise to the users who interact with their domain. We believe it would be a false and misleading trade practice to post the policy without the intent to comply in good faith. However, EFF is not in a position to enforce this promise or monitor compliance.

We embed a 3rd or 4th party domain that isn't DNT compliant. What are some solutions?

It's common for domains that want to be DNT compliant to embed scripts, images or CSS from other 3rd or 4th party domains. Often those domains are not DNT compliant. There are a few possible solutions:

In some cases, double-iframing the embed from your domain in order to strip Referer headers may be sufficient. Whether that is the case depends on whether the dataset the embedded domain gets as a result of your embed is an "anonymized dataset" as defined by the DNT Policy or not.

Proxying the embeds through a system you control to remove information like referrers and client IP addresses.

Ask the domain to become DNT Compliant and post the policy.

Wrap the embed in an interstitial iframe that gives the user a clear indication of the privacy consequences before loading it. MyTube is a preexisting example of this method, which works for YouTube videos.

Is retention of visited domain names permitted in Anonymized datasets?

A dataset is anonymized if it does not permit the reconstruction of the reading habits or activities of small groups of users. Sometimes, the fact that a user visited a domain reveals their reading habits, and sometimes it does not. For instance, recording that a user went to google.com, baidu.com, wikipedia.org, or nytimes.com would typically be permissible, since those domains publish incredibly diverse content. But recording that someone went to monster.com, erowid.org, bankruptcyhq.com, gruene-bundestag.de or nra.org would not be permitted, because the mere fact of visiting these sites may reveal a lot about the visitor's reading habits or activities.

What kinds of due dilligence are advisable for Section 3 ("OTHER DOMAINS")?

Sometimes website operators do not consider all of the contractors and affiliates to whom they might be transferring data. There are several kinds of parties to consider:

Embedded third parties: check the sources of third party scripts, images, CSS and other content on your site. You can analyze your site's source code, or use client tools like RequestPolicy, uBlock, Ghostery. Probably the most comprehensive auditing method is to use a combination of the default-src and report-only Content Security Policy directives; they provide a way to have visiting browsers report unexpected third parties to you automatically.

If the mere fact of visiting your domain does not reveal your visitors' reading habits (see the previous question):

Ensure that your hosting provider and CDN (if you have one) are not retaining the URLs or paths of requests to your site in association with IP addresses or cookies.

If visiting your domain inherently reveals users' activities or reading habits:

Ensure that your hosting provider and CDN (if you have one) do not retain IP addresses at all, or that they are bound in accordance with Section 3.

Ensure that your HTTPS deployment either uses OCSP stapling, or that your CA's OCSP service is bound in accordance with Section 3. Otherwise, the OCSP server may record your users' activities in violation of this policy.