KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

WHAT DOES "DO NOT TRACK" MEAN?

A SCOPING PROPOSAL BY THE CENTER FOR DEMOCRACY & TECHNOLOGY

January 31, 2011

Introduction

"Do Not Track" (DNT) is gaining momentum. In 2007, CDT and a coalition of other public interest groups called on the Federal Trade Commission (FTC) to create a Do Not Track system that consumers could use to avoid being tracked as they browsed the Web.[1] For three years, the idea went nowhere. Then, last July, FTC Chairman Jon Leibowitz expressed support for DNT in Congressional testimony.[2] In December, the FTC staff featured DNT in its draft privacy report[3] and a House subcommittee held a hearing on the topic.[4]

Most importantly, in recent weeks, two leading browser makers have announced plans to introduce DNT features into their browsers. This is particularly significant, both because the browser is the gateway to the Internet for most users[5] and because there is a strong argument that, even without any new legislation or regulation, websites and advertisers would have to respect consumer statements conveyed through the browser that they did not want to be tracked.[6]

Accordingly, it is time to define what "track" actually means in the context of DNT.

---

[1] *Consumer Rights and Protections in the Behavioral Advertising Sector* (Oct. 2007), http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

[2] Oral testimony of FTC Chairman Jon Leibowitz. Hearing Before the Subcomm. On Commerce, Trade, and Consumer Prot. Of the H. Comm. On Energy and Commerce, 111th Cong. (July 27, 2010), *available at* http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2010. Leibowitz did not include a discussion of DNT in his written testimony.

[3] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 57-63 (Dec. 1, 2010) *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[4] Do Not Track Legislation, Is Now the Right Time?: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. Of the H. Comm. on Energy and Commerce, 111th Cong. (Dec. 2, 2010), *available at* http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8127.

[5] Center for Democracy & Technology, Center for Democracy & Technology, *Browser Privacy Features: A Work in Progress, Version 3.0* (Dec. 2010) *available at* http://www.cdt.org/files/pdfs/20101209_browser_rpt.pdf.

[6] Section 5 of the FTC Act (and comparable state laws) prohibit deceptive or unfair business practices. If a consumer reasonably expects that a website that responds to DNT-tagged web requests will not track the user, the violation of the user's "terms of use" could well be interpreted as a deceptive or unfair practice.

Achieving consensus on this question will guide the development and implementation of browser-based DNT tools, serve as the basis for educating users about their options, and guide enforcement bodies, such as the FTC, as they consider the implications of the concept.

Defining Do Not Track requires first defining "tracking," and that is not easy. Technology and industry practices change quickly and future innovations may be impossible to predict. However, guidelines that are clear and appropriately flexible can both empower users and provide clarity for companies. Once the principles underlying the concept of "tracking" are well understood, development of efficient DNT mechanisms—and their predictable use by all entities on the Web–will more readily follow.

In this spirit, CDT offers this proposal as a preliminary effort to scope what "track" should and should not communicate in the context of browser-based DNT mechanisms.

We have drawn on definitions and ideas found in a diverse set of sources, including the[7] the FTC's online behavioral advertising self-regulatory guidelines,[8] Interactive Advertising Bureau's online behavioral advertising self-regulatory guidelines, Rep. Bobby Rush's 2010 consumer privacy bill (the BEST PRACTICES Act), [9] CDT's online advertising threshold analysis,[10] and documents that CDT has produced through its work in technical standards bodies.[11] In the coming months, CDT will be consulting with major browser makers, advertising networks, online publishers, privacy and consumer advocates, and others stakeholders.

The functional definition of what "track" means should apply regardless of how a browser actually implements a DNT solution. For example, Microsoft in December announced "Tracking Protection Lists"[12] as its mechanism to allow users to block tracking. To enable this mechanism, one or more trusted third parties (or the user herself) will compile a list of domains that "track" users. When a user imports a list to her browser, the browser will prohibit websites from sharing her contact with those tracking domains, thus prohibiting those domains from tracking the user across sites. Under this approach, those compiling lists will have to make the determination of what constitutes tracking in order to decide which domains to include on their lists. The definitions we seek to develop should guide those judgments.

Another way to implement DNT is for a browser to append a "Do Not Track" header to web requests of users who enable the option.[13] Mozilla announced in January that it intends to build

---

[7] Interactive Advertising Bureau, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

[8] Federal Trade Commission (Bureau of Consumer Protection), *Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology* (Feb. 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm.

[9] BEST PRACTICES Act, H.R. 5777, 111th Cong. (2009).

[10] Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), *available at* http://www.cdt.org/privacy/20090128threshold.pdf.

[11] Alissa Cooper, John B. Morris, and Erica Newland. Privacy Rulesets: A User-Empowering Approach to Privacy on the Web. In W3C Workshop on Privacy for Advanced Web APIs, London, UK, July 2010, *available at* ww.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html.

[12] Jordan Robertson, "Microsoft Unveils 'Do Not Track' IE Feature" (Dec. 7, 2010), *Associated Press, available at* http://www.msnbc.msn.com/id/40554324/ns/technology_and_science-security/

[13] Jonathan Mayer and Arvind Narayanan, *Do Not Track: Universal Web Tracking Opt Out*, *available at* http://donottrack.us/.

such an implementation into its Firefox browser.[14] Under this approach, it is incumbent upon individual websites to honor the header. This requires websites to evaluate whether they are tracking or not. Again, a clear definition of "tracking" would help define both user expectations and the practices of websites that engage in tracking.

Finally, while this draft discusses DNT solely in the context of data generated by web-based activities, the implementation of DNT should ultimately not be limited to Web activities. We urge the makers of mobile operating systems, for example, to empower users to express DNT preferences such that these will be transmitted to apps.

What Should "Do Not Track" Mean?

The user experience online involves the unintentional disclosure and commercial compilation of many different kinds of user data among different entities, comprising a wide range of practices that could be called "tracking." At the most basic level, online communication requires the exchange of IP addresses between two parties. Completion of e-commerce transactions normally involves the sending of credit card numbers and user contact information. Social networking sites often revolve around user-provided profiles. And much web content is supported by advertising. Much of this advertising is linked to either the content of the page visited or to a profile about the particular user or computer. Complex ecosystems have arisen around the online data flows.

CDT believes that DNT mechanisms should, at their most basic, empower users to prevent the collection and correlation of data about their Internet activities. Users expect control over who is tracking them and how tracking data may be shared. To that end, CDT offers the following provisional definition of "tracking": **Tracking is the collection and correlation of data about the Internet activities of a particular user, computer, or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or compliance with law enforcement requests.**

It is this understanding of "tracking" that frames the ideas and descriptions in this paper.

CDT does not believe that DNT is intended to enable users to block all advertising or prevent all data collection. CDT also believes that the collection and use of "actively shared" data–data that users knowingly and voluntarily provide in web forums, on social networking profiles, or on blogs or microblogs–is out of scope for DNT. While the consolidation and unexpected uses of this data can raise serious privacy concerns, CDT recommends that the collection and use of this data be addressed in other ways, such as through comprehensive consumer privacy legislation.

CDT instead recommends that DNT be narrowly scoped to address the collection and use of passively shared data. Users do not typically expect that records are being collected of the various sites and pages they visit across the web, particularly because such collection is often performed by companies that are not consumer facing. While a user might reasonably expect that individual websites can track them across that website, many users do not expect or want companies or their industry partners to be able to track what they browse and read across

[14] Julia Angwin, *Web Tool On Firefox To Deter Tracking*, THE WALL STREET JOURNAL, January 24, 2011, http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html.

multiple, unrelated sites.[15] It is this concern that should be the focus of DNT.

CDT also believes that a user's decision to enable a "Do Not Track" mechanism should be understood as an initial, and not necessarily final, indication of user intent. Even after a user has enabled a DNT mechanism, a website should still be able to ask, in a clear and conspicuous manner,[16] for the user's affirmative, express permission to track her, perhaps in exchange for better content or a reduced price for a certain service. For example, a news site could present a dialog box and request that the user grant permission to a certain ad network to track her on that site as a condition of service. Or a photo sharing site could offer users a choice during registration to host limited amounts of data for free or to host more if the users allow certain third-party tracking. On this theory, as long as the request for permission is clear and prominent and a user is given the opportunity to consider and make an informed choice about the value proposition, companies should be able to get a user's affirmative permission to ignore the generic "Do Not Track" instruction.

In short, when the user has affirmatively chosen to use a Do Not Track mechanism, all future tracking (as defined above) becomes opt-in.

In this document we present preliminary recommendations for which activities should be considered "tracking" for the purposes of DNT and which should not. We summarize these recommendations in the chart below.

Tracking	**Not tracking**
Third-party online behavioral advertising	Third-party ad and content delivery
Third-party behavioral data collection for first party uses	Third-party reporting
Third-party behavioral data collection for other uses	Third-party analytics
Behavioral data collected by first parties and transferred to third parties in identifiable form	Third-party contextual advertising
	First-party data collection and use
	Federated identity transaction data
	Data collection required by law and for legitimate fraud prevention purposes

What is "Tracking"?

As a stating point for defining DNT, CDT proposes that the following activities should be considered "tracking":

[15] *See* Joseph Turrow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), *available at* http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.
[16] FTC Privacy 2010.

- Third-party online behavioral advertising
- Third-party behavioral data collection for first party uses
- Third-party behavioral data collection for other uses
- Behavioral data collected by first parties and transferred to third parties in identifiable[17] form

This is certainly not a comprehensive list. Instead, it is meant to serve as a guide for implementing the spirit of DNT.

We describe these activities below.

Third-party online behavioral advertising

Today, many websites (commonly described as "first-party sites" or publishers) contract out both advertising and content to third party advertising and content syndication networks. These networks have the ability to place a unique identifier on a user's computer, which the network can subsequently recognize as the user moves from site to site. Using this identifier, the network can amass a profile of a range of sites visited by the user. For the purposes of this document, third-party online behavioral advertising means the collection of data about a particular user, computer, or device, regarding web usage over time and across non-commonly branded websites for the purpose of using such data to predict user preferences or interests and to deliver advertising to that individual or her computer or device based on the preferences or interests inferred from such web viewing behaviors.

Under this definition, the following would be considered third-party online behavioral advertising:

Example 1: An advertising network contracts with a number of websites to place web bugs (otherwise known as tracking pixels) on these websites in order to place HTML cookies on the devices of visitors to these websites. These cookies allow the advertising network to collect information about some of the websites the user visits in order to compile a profile to associate with that user's device. The advertising network uses this information to target advertisements to the user. Alternatively, the advertising network sells this information, along with an IP address, unique device ID, or other potentially identifying information to another advertising network that uses this information to target advertisements to the user.

Example 2: A social networking site employs iframes[18] on a wide range of non-commonly branded websites to embed content customized for the user.[19] In order to display the customized content on each website the user visits, the social network must receive the URL of each of these websites. The social network collects these URLs and uses them to target advertisements to the user. Alternatively, the social network collects these URLs and sells them to – or shares them with – an advertising network, along with user data that can be reasonably

[17] Data is in identifiable form if it can be reasonably linked to a specific consumer, computer, or other device. This is the definition provided by the FTC. *See e.g., supra* note 3*, supra* note 8.

[18] Using an iframe tag, a website can display an html document that is hosted on a third-party website. In essence, this first-party website grants the third-party website an "embassy" on its page. *See* http://en.wikipedia.org/wiki/HTML_element#Frames.

[19] An iframe alone, even when branded with the logo or name of a third-party company, is insufficient to render two websites commonly-branded.

linked to a specific user, computer, or other device. The advertising network uses this information to target advertisements to the user.

Example 3: A user visits the website of a furniture retailer and examines the specifications for a particular sofa. Alternatively, the user places this sofa in her online shopping cart but does not proceed to purchase the sofa. As the user navigates around the website, the furniture retailer permits a number of third-party advertising firms to place tracking cookies in the browser of the user. The fact that the user nearly purchased the sofa is used to target advertisements for the sofa on websites that are not commonly branded with the furniture retailer or on advertisements that show up when the user opens an application on her mobile device (This is one form of a practice commonly known as "re-targeting.").

Third-party behavioral data collection for first party uses

This practice refers to the collection of data about a particular user, computer, or device regarding web usage over time and across non-commonly branded websites, by a particular company for the purpose of using such data to advertise to or customize the products or services that the said company (or a commonly branded site) provides the user.

Under this definition, the following would be considered third-party behavioral data collection for first-party uses:

Example: An online portal website contracts with other websites to place web bugs on these websites and to place HTML cookies or other unique identifiers on the devices of visitors to these websites. These cookies allow the company to collect information about some of the websites the user visits. The company uses this information to customize the content on the online portal it provides for the user, the search results it presents when the user uses its search engine, or the advertisements it shows along those search results.

Third-party behavioral data collection for other uses

This refers to the collection of data generated by or derived from a particular computer or device regarding web-viewing behaviors over time and across a non-commonly branded websites, by a particular company. Collection for other uses may include offline marketing or market research based on aggregated tracking of a population of users. While the latter may raise fewer privacy risks than individualized targeting and profiling, many users may object to the tracking of their web usage for research purposes, and persons who uses a browser-based DNT mechanism would reasonably expect to be opting out of such tracking.

Under this definition, the following would be considered third-party behavioral data collection for other uses:

Example 1: A company contracts with popular websites to place web bugs on these websites and to use "browser fingerprinting"[20] to uniquely identify of visitors to these websites. This allows the company to collect information about some of the websites the user visits and associate that information with an identifier linked to a user's device. If the tracking company is able to discern the names of certain individuals from partner companies or from data entered by users

[20] Peter Eckersley, How Unique is Your Web Browser?, Electronic Frontier Foundation, https://panopticlick.eff.org/browser-uniqueness.pdf;

themselves into web forms, the company could use behavioral data about a user generated by web tracking to send direct marketing mail to that individual or otherwise market to that person.

Example 2: A company contracts with a range of websites to place web bugs on websites and uses HTML5 DOM storage store unique identifiers onto users' devices. This allows the company to collect information about some of the websites the users visit and associate that information with identifiers linked to those users' devices. The company eventually aggregates this data into a market research report detailing how a large population of web users surf the web.

Example 3: A company provides authentication services for publishers that run commenting systems. When the company authenticates a user, it retains a copy of the URL of the site that the user was logging in to. The company combines information from across sites to create a record of the sites at which it has authenticated the user. The company uses this data for purposes other than fraud prevention, such as for market research purposes.

Behavioral data collected by first parties and transferred to third parties in identifiable form

This category covers the collection of data generated by or derived from a particular user, computer, or device regarding web viewing behaviors over time on one website or across commonly-branded websites, by a particular company. This company then transfers that data to a non-commonly branded company in a form such that the data can be reasonably linked to a specific user, computer, or other device.

Under this definition, the following would be considered behavioral data collected by first parties and transferred to third parties in identifiable form:

Example 1: A large e-retailer collects transactional data from users as they peruse its website and commonly branded websites. The company runs an algorithm to determine which IP addresses it receives are "static" — that is, they persistently identify return users to that site. The company then associates passive web browsing activity of its site with the static IP addresses of those users. The company then sells this data to another company without aggregating the information. The second company then uses this data to deliver targeted advertisements or content to devices using those IP addresses on other websites.

Example 2: A user visits the website of a furniture retailer and sets up an account with the retailer, providing her email address: example@example.com. She then examines the specifications for a particular sofa or perhaps places this sofa in her online shopping cart but does not proceed to purchase the sofa. The furniture retailer sells to an ad network or data aggregator the fact that the person with email address example@example.com is interested in this particular sofa. (This is one form of a practice commonly known as "re-targeting.").

What is *Not* "Tracking"?

DNT should not be conceived as a blanket prohibition against collection or use of user data; nor should it be construed as a prohibition against all third-party advertising. As discussed above, CDT believes that "actively shared" data—such as data users provide on social networking

profiles, web forums,[21] and through registering for various accounts—is largely out of scope, even though the use of this data raises a separate set of privacy concerns. Similarly, the merging of offline data and actively shared or passively shared data is largely out of scope. Instead, CDT recommends that DNT should be implemented to focus on the collection of the transactional, or "passively shared," data that is created as users navigate the web.

A number of difficult distinctions remain. For example, web analytics and product improvement services may seem to employ passive tracking but do not raise the same privacy concerns if properly implemented. CDT suggests DNT does not cover certain practices in this category, even when these practices involve placing a uniquely identifier on users' computers. In these cases especially, users will simply have to trust that their DNT preferences are being honored.[22] Thus, in order to qualify as a non-tracking activity, we suggest that both the entity collecting data and the entity on whose website data is collected (if this entity has contracted with a data collector) should be required to provide in their privacy policy a clear, affirmative, accountable statement describing the purpose of their data collection and specifically disclaiming any "tracking" behavior.[23]

CDT proposes that the following activities should be considered "*not* tracking" for the purposes of DNT:

- Third-party ad and content delivery
- Third-party reporting
- Third-party analytics
- Third-party contextual advertising
- First-party data collection and use
- Federated identity transaction data
- Data collection required by law and for legitimate fraud prevention purposes

Third-party ad and content delivery

Most modern websites import content from other domains when rendering a page for a visitor. This content could be a widget displaying the weather or stock prices, or it could be advertising optimized and delivered by a third party. Even if a user has enabled a DNT mechanism, third parties should be allowed to deliver content and advertisements on first party sites so long as the third parties do not engage in the behavior described above as "tracking."

Under this definition, the following would be considered third-party ad content delivery:

Example: The front page of a sports blog contains an iframe displaying scores from a partner (but third-party) site, and a banner ad delivered by a third-party ad network. The banner ad

[21] While we believe this is outside the scope of DNT, actively shared data can still be collected in ways that pose significant privacy risks. *See Julia Angwin and Steve Stecklow, 'Scrapers' Dig Deep for Data on Web, THE WALL STREETJOURNAL, October 12, 2010,* http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html

[22] For example, with the "do not track" HTTP header, consumers have to trust that the parties they are interacting with are respecting the header's direction. With the "block list' approach, consumers have to trust that sites not on the block list (or on a "white list" or "allow list") are not actually tracking them.

[23] We further recognize that an audit requirement, perhaps in a baseline consumer privacy law or related rulemakings, may ultimately be necessary in some situations – such as for those companies that drop unique identifiers – to ensure that tracking preferences are being honored.

shows advertisements that are targeted to the content of the page and not any particular visitor. Both third parties need the IP address and other basic information about the device requesting the content so that the ad can be delivered to the user. However, neither third party uses the information received about the device for any of the tracking purposes described above.

Third-party reporting

Third-party reporting refers to the logging of ad or content views by a third party for the purposes of identifying when a user interacts with a particular advertisement (or other content) and limiting the number of times a particular ad (or other content) is shown to a particular user. In order to optimize third-party ad and content delivery, a third-party company may place a unique identifier on a user's device in order to record data about the user's engagement with the third-party. As long as this unique identifier is only used to collect information about the user's views or interactions with the advertisements or content delivered by the third party (and not the first-party content), this would not be considered a tracking activity.[24]

Under this definition, the following would be considered third-party reporting:

Example: A news website contracts with a third-party ad network to deliver non-behaviorally targeted ads to site visitors. The ad network places a unique HTML cookie on visitors' computers in order to count unique visitors and in order to ensure that visitors do not see the same ad over and over. As long as the data collected about the user is exclusively about the advertisements themselves and is not tied to the first-party site that the user visited, this activity would not be considered "tracking."

Third-party analytics

Many websites also use third-party analytics packages to evaluate traffic on their own websites. Although this analysis may be conducted by a third party, the information delivered to the first-party website is exclusively about traffic on that site. As long as the third-party analytics provider does not aggregate or combine information across multiple sites or use the information for its own purposes, its practices should not be considered tracking.

Under this definition, the following would be considered third-party analytics:

Example: A company provides an analytics package for users who run their own websites. The analytics package directs visitors' browsers to contact the company's servers and the company reports an analysis of the log data. The user's collection and use of this data falls under the category of "first-party data collection and use." This is not a tracking activity. If the company that offered the product collects this data but neither augments data about individual site visitors in a manner that renders this data identifiable nor links it to data that has been collected through a "tracking" activity, then this is not "tracking" for the purposes of DNT.

Contextual advertising

[24] Ad impressions can be tracked using methods other than cookies with unique identifiers. Some could argue that DNT should never allow third-party cookies with unique identifiers to be placed on users' computers. CDT is interested in exploring ways to prevent fraud and to track ad delivery and impressions without using third-party cookies with unique identifiers.

The delivery of advertising based on the content of a webpage, a search query, or a user's contemporaneous behavior on a website without regard to activities of the user or her computer or device on non-commonly branded websites.

Under this definition, the following would be considered contextual advertising:

Example 1: A user is reading an article on the web about new smart phones and an advertisement for a smart phone is displayed alongside the article. The decision to display the advertisement was not influenced by any interest profile or record of its activity on other, non-commonly branded websites.

Example 2: A user initiates a search engine query for "movie theaters in Washington, DC." Alongside the search results, advertisements are shown for an Academy Award-nominated movie and restaurants that are located near a popular movie theater in Washington, DC.

Example 3: A user in Washington, DC uses a search engine to search for "movie theaters." The search engine is able to guess, from the users IP address, that the user is located in Washington, DC and displays content and advertising that is tailored to the DC-area.

First-party data collection and use.

Generally speaking, first-party data collection and use should not be considered "tracking" for the purposes of DNT. When the first party sells user data that can be reasonably linked to a specific user, computer, or other device, however, this activity does not fall under the category of "first-party data collection and use." Instead it falls under the category of "behavioral data collected by first parties and transferred to third parties in identifiable form," which we classify as a tracking activity. Similarly, when the first party combines data acquired through a "tracking" activity with data obtained through a tracking activity, any use of that combined data becomes a "tracking activity."

More specifically, first-party data collection and use refers to the collection of data generated by or derived from a particular computer or device regarding web viewing behaviors or web-transmitted precise location data, over time and across commonly-branded website or websites, by a particular company for the purposes of delivering first-party behavioral advertisements or otherwise customizing content on a website that is under the same common branding.

Under this definition, the following would be considered first-party data collection and use:

Example 1: An e-retailer recognizes return visitors using cookies or account logins. The e-retailer uses only past purchases the visitor made on its website, past webpages she visited within its website, log data,[25] and gender information visitor provided in her user profile to customize the content displayed to the visitor on the sites homepage or the advertisements the visitor sees as she traverses the website.

[25] Log data includes data such as: IP address; browser type, version, and operating system; screen size; technologies, fonts, and audio formats supported by the browser; URL of the page that directed the visitor to the site; whether the visitor has bookmarked the website on the web browser; the webpages within the site that the visitor visits, the webpage the visitor visit first on the site (the entry page), and the webpage the visitor visits last on the site (the exit page); bandwidth used; the amount of time the visitor spends during a visit to the site; the time and date of your site visit.

Example 2: A company offers a search engine and a social networking site; the services are commonly branded. The search engine customizes search results and the advertisements adjacent to the search results based on the user's social networking profile, location, past uses of the search engine, and – of course – the search terms themselves. The search engine does not use data from third parties to customize the results or ads, nor does it use data collected by tracking the user on non-commonly branded websites.

Federated identity transaction data

Websites are increasingly outsourcing user registration and authentication processes to third-party identity providers. These identity providers have a unique vantage point from which to passively log users' registration and authentication activities over time and across an array of different contexts.[26] Use of this data by an identity or authentication provider should be limited to statistical reporting to a relying party (here, the website) in connection with the activity on that website. As with third-party analytics, as long as the data collected by the third-party are not aggregated or merged across non-commonly branded sites and domains, that activity should not be considered tracking.

Under this definition, the following would be considered a federated identity transaction:

Example: A popular portal offers to its registered users the ability to log into a wide range of other, third-party sites by authenticating to those sites its users' online identities. The portal keeps track of the third-party sites that a user logs into using the portal's authentication; however, it does not customize content or advertising on the portal's own sites based on the information, or use or transfer this information for any purposes other than offering identity-management services to its users.

Data collection required by law and for legitimate fraud prevention purposes

Data is retained for fraud prevention purposes or for purposes required by law and is not used for any "tracking" activities.

Under this definition, the following would be considered data collection for legitimate fraud prevention purposes:

Example: An advertising network retains for 90 days logs of the IP addresses of all users who has clicked on a particular ad for fraud prevention purposes. The advertising network does not combine the IP addresses with information about individual site visitors in order to create profiles about these visitors. The advertising network also does not sell or otherwise transfer these IP addresses.

Conclusion

With browser developers unveiling DNT mechanisms, it is now essential to seek consensus as to what an affirmative consumer statement—"do not track me"—actually means. Once consensus has been reached, users can understand what to expect from DNT, and companies

[26] The availability of this data to the identity provider is not inevitable; it depends upon the implementation of the underlying authentication protocols.

can know how to implement it. This proposal is a contribution to this discussion.

Though not specifically discussed here, DNT could also be a powerful idea in the context of mobile apps and other non web-based interactions. These and other contexts should be carefully considered on their own merits.

It is also important to emphasize that DNT does not "fix" privacy. DNT is a privacy-enhancing technology that can help return some control to users with respect to certain types of tracking behaviors of which they may not approve. A baseline, comprehensive privacy bill that provides substantive protections for users is still necessary to fully protect users, promote trust in the online environment, and position the U.S. as a global leader as other countries rapidly work to update their own privacy regimes.

As we continue to refine the ideas and descriptions presented in this paper CDT will be consulting with relevant stakeholders. We welcome any comments, questions, or concerns.

For further information, contact:

Justin Brookman
Director, Consumer Privacy Project
202-637-9800
justin@cdt.org