July 16, 2013

Explanatory Memorandum for Working Group Decision on "What Base Text to Use for the Do Not Track Compliance Specification"

Table of Contents

This Explanatory Memorandum accompanies the decision of the Working Group of July 15, entitled "What Base Text to Use for the Do Not Track Compliance Specification."[1] The decision was written by Matthias Schunter and Peter Swire, co-chairs of the Tracking Protection Working Group of the World Wide Web Consortium ("W3C"), in accordance with long-established procedures in the Working Group. That decision of the Working Group addresses the question of what base text to use for the Do Not Track Compliance Specification, and concludes that the draft put before the group in June ("June Draft") will be the base text rather than the proposal submitted by the Digital Advertising Alliance and other group members ("DAA Proposal.")[2] Part I of this memorandum provides history and background of the process to date, with emphasis on the issues that differ between the two texts.[3] Part II is called "Do Not Target," and discusses the definition of "tracking," the means of user choice concerning targeted online advertising, and related topics. Part III is called "Do Not Collect," and addresses issues including minimization of data collection and the use of unique identifiers. Part IV is called "Data Hygiene." It examines a range of controls that a company may apply to de-identify data and reduce the risk that data is revealed without authorization. Parts II to IV include discussion of many of the comments submitted under the July 12 deadline concerning which base text to adopt. Part V addresses additional comments submitted, responding especially to comments that supported the DAA Proposal to become the base text.

I: **History and Background**

A. Early history of DNT and Formation of the Working Group

One early source of the Do Not Track idea was a 2007 paper "Consumer Rights and Protections in the Behavioral Advertising Sector."[4] The paper was signed by ten consumer groups, including the Center for Democracy and Technology and the Electronic Frontier Foundation, who today are active members of the Working Group. The paper called for creation of "a national Do Not Track List similar to the national Do Not Call List." The paper touched on a number of the issues that have since occupied the Working Group, including on the current issue of unique identifiers: "Advertisement from servers or other technologies that do not employ persistent identifiers may still be displayed on consumers' computers. Thus, consumers who sign up for the Do Not Track List would still receive advertising."

In February 2009, after a process of public workshops and comments, the Federal Trade Commission published a Staff Report on "Self-Regulatory Principles for Online Behavioral Advertising."[5] After reviewing calls for a Do Not Track approach, the Staff Report stated: "FTC staff believes that companies should provide consumer choice for the collection of data for online behavioral advertising if the data reasonably could be associated with a particular consumer or with a particular computer or device." At least partly in response to this report, deployments of Do Not Track technology in browsers began in late 2010. In early 2011, W3C received a Member submission from Microsoft, proposing standardization of a Do Not Track signal and Tracking Protection Lists. An April 2011 workshop on Web Tracking and User Privacy at Princeton brought together almost a hundred diverse participants, out of which was chartered the Tracking Protection Working Group. That summer, European Commissioner Neelie Kroes called for prompt industry standardization of Do Not Track.[6] The Working Group first met in September 2011. Matthias Schunter (then IBM, now Intel) was chair of the Tracking Preference Expression ("TPE") Specification, to define the technical mechanisms for expressing a DNT preference. Aleecia McDonald (then Mozilla, now Stanford) was chair of the Tracking Compliance and Scope ("Compliance") Specification, to define the meaning of a DNT preference and set out practices for Web sites to comply with this preference. The First Public Working Drafts for both parts were published in November 2011.

In January 2012 the European Commission hosted a Face-to-Face meeting of the Working Group in Brussels, with addresses by Commissioner Kroes and then-FTC Chairman Jonathan Leibowitz. The next month, the White House and the FTC held an event about consumer privacy. Major browsers agreed to build DNT capabilities into their browsers. Also participating were the DAA and its member organizations, including the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, the Interactive Advertising Bureau, and the Network Advertising Initiative. The DAA said: "Today the DAA announced that it will immediately begin work to add browser-based header signals to the set of tools by which consumers can

express their preferences under the DAA Principles. The DAA expects that such functionality will be implemented within nine months."[7]

In March 2012, the FTC issued its report on "Protecting Consumer Privacy in an Era of Rapid Change."[8] The Commission stated its belief that "any Do Not Track system should include five key principles. First, a Do Not Track system should be implemented universally to cover all parties that would track consumers. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction."

Also in that March, the group published new, more substantive drafts, with differing options on different sections. Through the summer it debated topics of breadth of parties and permitted uses for data otherwise prohibited by the Compliance Specification. In June, the group reached consensus on not sending DNT signals by default. For the more technical work, TPE specification, the group made decisions on use of a tracking status resource and an optional response header in order to communicate tracking status back to the user and to be silent on user agent requirements for equal effort on three possible choices.

The Working Group continued to grow in size through the fall of 2012, including more representatives from advertising industry companies and self-regulatory organizations. The Working Group met in Amsterdam in October, including discussion of interaction with EU data protection regulations, and W3C held a broader DNT-related workshop in November.

B. <u>History Since Change of Co-Chair</u>

In November 2012, Peter Swire succeeded Aleecia McDonald as co-chair of the Working Group, leading the group's efforts on the compliance specification. In order to get up to speed as he entered the group, Swire requested overview comments from participants, and conducted dozens of meetings with stakeholders. In January 2013, Swire chaired his first in-person meeting in Washington, D.C., focused on de-identification. The invited presenter for this meeting was Dr. Khaled El Emam, a Canadian de-identification expert who has recently published a book on the subject.[9] The meeting invitation asked stakeholders to send technically sophisticated participants. Since that time, the Working Group has worked intensively on the issue of de-identification. An important reason for this focus has been a consensus in the group that data at some point is scrubbed enough so that data becomes out of scope of the DNT specification. Put another way, data at some point is de-linked or de-identified enough that use of it does not count as "tracking." In drawing the line between in-scope and out-of-scope, a major privacy concern is that data might be re-identified. Therefore, more scrubbing creates less risk for individuals. A major

industry concern has been to retain the utility of data, and more scrubbing generally means lower usefulness for industry.

i. February 2013 Face-to-Face

At the Face-to-Face in the Boston area in February, 2013, the opening session began with a request to the group to work with decorum and assume the good faith of other participants. Swire reports that the group has consistently acted in this way since he began work with W3C, and thanks the group for its hard work and professional tone. Swire proposed five criteria for the standard:[10]

1. The group should create a W3C standard. Discussions in the group often overlap with discussions in other venues, and decisions in the group should be informed by those other discussions, but the task of the Working Group is to create a standard within the W3C process.
2. The standard should be consistent with the group's charter.[11]
3. The standard should achieve a significant change from the status quo. The hard work of the group is intended to change and upgrade practices on the Internet with respect to tracking protection.
4. We should be able to explain why DNT:1 reduces tracking for participating sites. The reasonable aspiration is that user agents, including the major global browsers, will implement the DNT standard for many millions of users. We wish to be able to explain what it means to turn on DNT to users with widely varying levels or technical sophistication. In addition, one sign of an effective standard is that its effects can be communicated succinctly and accurately.
5. Adoption. As with any standard, we expect greater benefits in practice with higher adoption. A major reason to engage in standards work is to achieve inter-operability, in this group between users and user agents sending the DNT signal and sites receiving it.

These five criteria were discussed in the group. Although there has not been a formal consensus decision by the group to adopt them, there was little or no objection to them as stated and they have been referred to on multiple occasions since then as criteria for success. This chairs' decision treat the five criteria as important measures for what the Working Group is seeking to achieve.

The break-out sessions in Boston focused on two topics, "lifetime browsing history," essentially on the topic of de-identification, and the idea of "buckets" or "low-entropy cookies," essentially on ways to avoid the use of unique identifiers. Significantly, the two sessions correspond to the main two ways that the DAA Proposal contemplates handling browsing history. "Lifetime browsing history" is a forerunner of the DAA's current de-identification/de-linking approach, and the "buckets" proposal is a forerunner of the DAA's current aggregate scoring approach.

Lifetime browsing history. The topic of lifetime browsing history grew out of a proposal by Mike Zaneis of the Interactive Advertising Bureau, although the name came from Swire. The goal of this breakout was to explore if there is a feasible way to create an internet experience where a user's long-term pattern of browsing would not be associated with a unique identifier. For instance, a site might retain a truncated URI, such as newspaper.com, rather than a detailed URI, such as embarrassing-story-read-on-newspaper.com.

Obscuring the details of a user's reading on the internet matches closely with the work of leading privacy experts. Julie Cohen in the 1990's expressed the idea of a "right to read anonymously."[12] Neil Richards recently has developed the concept of "intellectual privacy," emphasizing how free speech values are protected if a user's reading history is kept confidential.[13] These authors emphasize the importance of a safe zone where individuals can develop their personality and their view of the world without fear of surveillance. A related concern is that databases of detailed URIs could be used by governments to look back through a person's internet usage, including to identify and potentially act against those who disagree politically with the government.

At the Face-to-Face, the group was unable to reach consensus on an approach to protect lifetime browsing history. Members of the advertising groups emphasized that detailed URIs were needed for an extended time for permitted uses, including:

1. Security and fraud detection. In Boston and subsequently, some members of industry have stated that data might be needed for a time measured in years for security purposes.[14] Members of the group that objected to this time length emphasized the possibility of graduated response, with increasing use and retention of identifiable data where a problem is identified.[15] The group has not reached consensus on the need or desirability of routinely holding detailed URIs for security and anti-fraud purposes, especially for longer than a year.[16]
2. Proof that advertising was delivered as contracted for. The Metrics Review Council typically expects data to be retained for a year to prove that an advertising campaign delivered the promised ads. According to a subsequent invited talk to the group by the President of the MRC, the MRC has waived this requirement when asked to do so for privacy reasons.[17] The group has not reached consensus on the feasibility of depending on such waivers to shorten retention times generally.
3. Accounting and auditing. Chris Mejia of the IAB said that detailed records needed to be retained for up to seven years under the Sarbanes-Oxley Act.[18] In March, two invited speakers from Deloitte & Touche, a global accounting firm, briefed the group on the rules for when detailed records should be retained for accounting and auditing purposes.[19] The group has not reached consensus on the need for large-scale retention of detailed URIs for these purposes.[20]

In Boston and subsequently, the group has not been able to reach consensus on a lifetime browsing history approach. A major reason is skepticism on the part of consumer advocates that there would be a meaningful reduction in the long-term retention of detailed URIs. Consumer advocates pointed out that industry was claiming the need to hold the details for multiple years for security, accounting, and other permitted uses.[21] Industry also stated that the same physical database would be used for marketing purposes (with detailed URIs suppressed) and for the permitted uses (with detailed URIs retained).[22] Access controls would enable access for the permitted uses but not for marketing purposes.[23] Because a proposal based on deleting "lifetime browsing history" would in fact retain detailed browsing history for the permitted uses, multiple consumer advocates concluded that they could not support this approach.

Buckets or low-entropy cookies. The other break-out topic in Boston was called "buckets or low-entropy cookies." This discussion featured major issues that are central to the decision today, including Do Not Collect, unique identifiers, and the aggregate scoring portion of the DAA proposal. The basic idea was to see if there was a way to put users into fairly large "buckets" of people with similar interests. In that way, industry could send targeted advertisements, and privacy could be protected because the user would receive the advertisement as one person in a group, rather than as a targeted individual.

One source for this discussion was the EFF/Mozilla/Stanford proposal, made on June 6, 2012.[24] Under this proposal, the group would have a minimum size of 1,024 – a somewhat arbitrary number but one that the proponents thought was large enough to protect privacy. The proposal also contemplated a different technology than the current type of cookies. This "low-entropy cookie" would provide the site with enough information to place a user into a group, but not enough information to uniquely identify the user. The proposal did not specify a particular technology, but the Working Group has repeatedly referred to low-entropy cookies as shorthand for technologies that would allow targeting to members of a group but without the site being able to uniquely identify the individual user. The EFF/Mozilla/Stanford proposal thus highlighted two themes that regulators and consumer advocates have consistently stressed: (1) limits on collection of information ("Do Not Collect"); and (2) limits on the use of unique identifiers.

Members of the advertising industry expressed openness to targeting ads to groups rather than individuals.[25] Indeed, the aggregate scoring portion of the DAA Proposal appears to do precisely that – a company would collect information about a user's browsing and convert that into scores about "vacation in Hawaii" or "interest in purchasing a car." Under the DAA proposal, the company would generally use a unique identifier cookie to update a user's scores as new browsing occurred. Under the proposal, the company would also separate the browsing history from the score, in order to break the link between the targeted advertisements and the user's browsing history.

In Boston and since then, the group has not reached consensus on a way to use buckets or low-entropy cookies, despite extensive discussion. The advertising industry has said it would continue to rely on unique identifier cookies to target advertisements;[26] consumer advocates have objected to the use of unique ID cookies.[27] The advertising

industry has said that it would continue to collect the information it collects currently;[28] consumer advocates and others have said that a meaningful standard should include a Do Not Collect component.[29] Technical experts have stressed the availability of various methods to move away from unique identifier cookies;[30] the advertising industry, including its technical experts, have said that changing the system is a non-starter.[31] In addition, the DAA proposal specifically eliminates language in the June Draft that says that targeted advertising would shift to a system without unique identifiers, if that were reasonably available.

In conclusion on the Boston Face-to-Face in February 2013, the group engaged in detailed discussions of major issues that separate the DAA Proposal and the June Draft, including de-identification, Do Not Collect, the role of unique identifiers, and the use of aggregate scoring. The group has honed its understanding of these issues since Boston, but these key issues have remained quite similar.

ii. Between the Boston and Sunnyvale Face-to-Face Meetings

Between the Boston Face-to-Face in February and the Sunnyvale Face-to-Face in early May, the Working Group in the weekly calls addressed numerous issues that could go into a final compliance standard. For instance, the group addressed definitions such as for "first party," "multiple first parties," and "service providers." We considered issues about user interface and user education, seeking to bridge browser and advertiser perspectives on how a Do Not Track choice should be presented to users. We discussed whether to include limits on the abilities of first parties to append offline data to data collected online. We did extensive work on the issues of market research and audience measurement, resulting in a detailed industry proposal governing how data could be used for audience measurement purposes. We continued to work on the issues raised in Boston, such as de-identification and the length of time data would be retained for different permitted uses. There were also extensive discussions among Working Group members, both with and without Swire's participation, to find consensus on the group's work.

iii. Sunnyvale Face-to-Face

The Face-to-Face meeting in Sunnyvale, California in early May used the "Draft Framework" as its agenda.[32] Along with continued work on the other major issues, the Draft Framework contained proposals designed to ensure that the DNT signal would be off by default.[33]The Sunnyvale meeting concluded with a "Consensus Action Summary," which stated that "there was sufficient progress during the meting to merit moving ahead with the Do Not Track standard toward the July 2013 Last Call deadline."[34] The Sunnyvale meeting did not, however, result in an overall consensus of how to bridge the group's differences on issues including de-identification and the use of unique identifiers.

The Draft Framework emerged from discussions among diverse members of the Working Group. DAA General Counsel Stu Ingis gave the initial presentation of the Draft Framework on a call on April 29.[35] As explained by Swire in the May 1 weekly call, the Draft Framework emerged from discussions that included the DAA as well as browsers, some

consumer groups, and regulators.[36] The Draft Framework was used as the agenda for the Sunnyvale meeting, and its specific items were understood as a draft overall approach rather than as a sign-off by any stakeholder on each specific provision.[37]

Much of the discussion at Sunnyvale addressed Part 6 of the Draft Framework, defining what it would mean for DNT to be off by default:

1. Browsers and not other user agents. The Draft Framework stated that this round of DNT work would apply to browsers but not other user agents. Some members of the group objected to this proposal, citing the difficulty of technically defining a "browser" and expressing concern about the effect on tracking of mobile devices.[38]
2. No DNT on install. The Draft Framework stated that the browser choice setting would be available in the browser settings panel, and not through an installation process or other similar mechanism. There was no consensus on placing this sort of limit on how the DNT user choice would be presented.
3. Measures to make sure only the user sets DNT:1. The Draft Framework called for a combination of technological and non-technological measures to greatly reduce the risk that anyone other than consumers set the choice about DNT. Advertisers were concerned, for instance, that the DNT signal might be turned on by anti-virus software, other software, routers between the user and the site, or in other ways. The discussion in Sunnyvale revealed considerable skepticism in the group that effective measures could be developed to detect and prevent the DNT signal from being turned on in these ways.[39]
4. Brief and neutral description of what the signal means. The group did have productive discussions including browsers and advertisers about how to communicate to users on topics including "the fact that if the browser choice setting is activated it limits collection and use of web viewing data for certain advertising and other purposes."[40]

The importance of these discussions about default settings in Sunnyvale has become clearer in retrospect. While explaining the DAA proposal to the group on July 3, IAB General Counsel Mike Zaneis said "My members (now seeing 20-25% of user base sending DNT flag. Early on, our position had been: perhaps the W3C could standardize the DNT signal, and we would treat that as an industry opt-out. That is no longer tenable. We expect DNT:1 signals to approach 50% in the short-term."[41] Instead of providing an industry opt-out, the DAA Draft is "[m]ore of a data hygiene practice." [42] Similarly, Shane Wiley of Yahoo has explained recently why it is so difficult to have measures to ensure that it is the individual user who chooses to turn on DNT: "The ease at which injecting the DNT:1 signal in headers (Mozilla states it took only 13 lines of code), the lack of technical mechanisms to ensure this only occurs by user action, and the proliferation of signals coming from browser add-ons, privacy tools, anti-virus applications, network intermediaries such as WiFi access points and routers, and others, leads many technical experts on all sides of the table (consumer advocate, browser vendor, and industry) to predict DNT:1 rates above 50% - possibly even above 80%."[43] After the Sunnyvale

meeting, the focus of the advertising industry work has shifted away from efforts to address the default issue. Instead, the DAA Proposal assumes a high rate of DNT:1 signals, and the DAA proposes actions that its members are prepared to take in this high-rate environment.

Apart from the default and user interface issue, the Consensus Action Summary at the end of the meeting addressed three issues:

1. Audience measurement. The group agreed to continue work on a proposed permitted use for audience measurement, including "to try to find audience measurement language that can substitute for the DAA's market research exception."
2. De-identification and retention periods. The group agreed to examine a three-state de-identification process, called "red" (raw data), "yellow" (some identifying data removed), and "green" (de-identified and de-linked enough that the data becomes out of scope of the DNT standard). Shane Wiley presented a version of a three-stage approach that closely resembles the de-identification and de-linking proposal in the DAA Proposal. The group asked questions about Wiley's approach, but there was no consensus that it was the group's approach to the issue.
3. Unique identifiers. The Summary stated: "There will be ongoing discussions of unique identifiers as a critical issues for advocates."

iv. The Process Since the Sunnyvale Face-to-Face

The Consensus Action Summary at Sunnyvale said that the group would continue to work toward the July 2013 Last Call deadline. The work of the group has been shaped by the goal of achieving Last Call by the end of July, or, failing that, to bring enough clarity to the process that the group can assess by the end of July whether and how to proceed. Today's decision seeks to summarize the chairs' views of the process on key open issues in the compliance specification, in order to assist in that assessment.

The June Draft was issued on June 10.[44] In contrast to the previous Editors' Draft,[45] the June Draft contained one option for each of the areas where the previous draft had multiple options. In circulating the draft, Swire wrote: "Working closely with W3C staff, and based on numerous discussions with members of the WG, this June Draft is my best current estimate of a document that can be the basis for a consensus document in time for Last Call."[46] The group was invited to submit proposed amendments to the June Draft, called "change proposals," by June 26.[47] On the weekly teleconference that day, the authors of the change proposals were invited to describe them briefly,[48] and Shane Wiley presented more detail about the red/yellow/green de-identification approach that he stated was consistent with the DAA's submission that day.[49]

On June 28, Swire sent the group an "initial work plan on change proposals," which highlighted three main areas of work, which match closely with the topics of today's decision: (1) de-identification; (2) identification and unique identifiers; and (3) the DAA

Group proposal.[50] With respect to the DAA's submission, Swire specifically asked the Working Group to prepare to state their views on the DAA Proposal: "With a presentation of this integrated package, the group can ask questions to clarify the multiple proposed changes, and begin a process of identifying areas where others in the group may agree to the proposal, or an amended version of the proposal, or else articulate reasons why they would not join a consensus on the proposal."

On July 2, Swire notified the group that they should prepare comments on the topic of today's decision, choosing between using the June Draft or the DAA Proposal as the base text for continued work in the group.[51] In addition to the issues of de-identification and unique identifiers, this email pointed out that the DAA Proposal "makes specific choices on the definition of tracking and the scope of first and third party compliance." Consistent with the Working Group's longstanding decision policy, used previously on September 14, 2012,[52] friendly or perfecting amendments to the DAA proposal were due by July 9. On July 3, after the weekly call, co-chairs Schunter and Swire provided more detail about the current process.[53] The DAA Proposal was the topic of detailed discussion on the weekly calls on July 3 and July 10, including responses to questions posted to the public mailing list. The Working Group email list was filled during this period with literally hundreds of posts, many of them being explanations or comments from representatives of companies or organizations that have signed onto the DAA proposal.[54] Formal objections to using either the June Draft or the DAA proposal were due at close of business on July 12.

In conclusion on the history of the group since the Sunnyvale Face-to-Face, there has been detailed and repeated consideration by the group of precisely the issues raised as different between the June Draft and the DAA Proposal. Today's decision is based on the Working Group's record both before and since the Sunnyvale Face-to-Face, including the weekly teleconferences, emails to the public list, change proposals, and formal objections filed by July 12.

II. **Do Not Target**

Many public discussions about the Do Not Track standard have stated the main disagreement as "Do Not Target vs. Do Not Collect." For instance, Sarah Branham wrote in AdAge in early 2012: "From the marketing industry's perspective, do not track reads more as do not target,"[55] while the FTC and consumer groups have stressed Do Not Collect.[56] This Part of the Explanatory Memorandum discusses Do Not Target, including the definition under ISSUE 5 of "tracking" and the definition under ISSUE 16 of "collecting, sharing, using, and retaining data." Part III addresses Do Not Collect, including ISSUE 188 on unique identifiers.

A. The DAA Self-Regulatory Program and Do Not Track

The DAA implements its version of Do Not Target through its self-regulatory program, defined principally in two documents: "Self-Regulatory Principles for Online Behavioral Advertising," published in July 2009,[57] and "Self-Regulatory Principles for Multi-Site Data," published in November 2011.[58] The current web page for the program

describes the user choice this way: "When you see the AdChoices Icon on a Web page or near a Web banner, it lets you know that information used to infer your interests is being gathered or used to improve the ads you see. By clicking on the AdChoices Icon, you learn about how interest-based ads are delivered to you. More importantly, the AdChoices Icon gives you the ability [to] control whether you receive interest-based advertising and from which companies."[59] (emphasis added) Although members of the Working Group may differ in their views about the scope of the control tool, the ability for the user to control whether to receive targeted ads is what is meant by Do Not Target.

The DAA and its representatives have written extensively about the positive aspects of its notice regime (the AdChoices Icon) and choice regime (the ability for the user to opt out of interest-based advertising). In 2013 congressional testimony, Lou Mastria of the DAA stated that the DAA Principles "provide consumers with clear transparency, choice, and understanding about how their data will and will not be used." [60] Mastria continued, "23.5 million consumers have visited the DAA sites to learn about their advertising data choices," and "[t]he icon is served over one trillion times each month."[61]

On the other hand, consumer groups and others have stressed limitations of the DAA's self-regulatory program. In response to Lou Mastria's testimony, Justin Brookman of the Center for Democracy and Technology (CDT) pointed out four flaws in the current DAA program.[62] First, the DAA program only applies to members of the DAA. "Companies that don't sign up and pay for membership are not included, and receive no indication that a user does not want to be tracked." Second, the opt-out is cookie-based and is deleted whenever users delete their cookies. (The DAA program does provide a browser plug-in to make the opt-out persistent (not deleted with other cookies), but installing the plug-in is a separate step from the opt-out.) Third, the DAA Program stops targeted advertising but not the tracking of users. Fourth, the user interface of the DAA Program is confusing to users.

The level of opt-out has also been the subject of varying views. While Lou Mastria highlighted the 23.5 million users who have visited the DAA site, Justin Brookman highlighted adoption by fewer than 2 million users as of April, 2013, out of over 300 million people in the United States.[63] Critics of the self-regulatory program have observed that this opt-out rate of less than 1% is less than consumer sentiments about tracking recorded in public polling.[64] Supporters of the DAA approach, by contrast, have said that visitors to the DAA site, once informed about the nature of interest-based advertising, often decide not to opt out.[65]

The DAA participated in the White House and FTC event in February 2012. The DAA statement said: "Today the DAA announced that it will immediately begin work to add browser-based header signals to the set of tools by which consumers can express their preferences under the DAA Principles. The DAA expects that such functionality will be implemented within nine months."[66] The following month, the FTC reported on its understanding about Do Not Track: "the browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the

browser tools."[67] The browser tools, and the meaning of compliance with them, were immediate and ongoing topics for discussion within the Working Group.

The use of the Do Not Track signal to trigger Do Not Target was clearly contemplated by the Draft Framework, which was the agenda for the Sunnyvale Face-to-Face in May 2013.[68] Part 2 stated: "Non-compliance with DNT would be a DAA violation." Part 5 said: "We would determine a way to have the DAA codes become a way for compliance with the W3C syntax," with modifications to the DAA codes to add privacy protections in Part 1 (third parties would not collect "tracking data") and Part 3 (tighten DAA exceptions including market research and product development). The Draft Framework thus contemplated that Do Not Track would include at least the Do Not Target provisions in the current DAA Code, with mention of certain collection limits as well. As discussed above in the history discussion, this Draft Framework was presented to the Working Group by DAA General Counsel Stu Ingis in a teleconference on May 1. Its specific items were understood as a draft overall approach rather than as a sign-off by any stakeholder on each specific provision.

B. The Definition of "Tracking" and Related Terms Prior to the Current DAA Proposal

Defining the term "tracking" is obviously an important aspect of defining the meaning of "Do Not Track." At the outset, some context will aid understanding of the definitions of tracking in the June Draft and DAA Proposal. It is significant that what is often called the "Do Not Track" process is the topic of the "Tracking Protection Working Group." The group's name is important – this process cannot give users the choice to stop everything that a user might consider tracking. Instead, the criteria for success for the Working Group, as discussed elsewhere in this document, include significant protection from tracking.

It is not technically feasible to stop each thing that a user might consider tracking on the Internet, and users have reasons not to want to stop each thing. For instance, much as you need a person's telephone number to complete a call, a web site needs to know the user's IP address to deliver a web page. Users expect their information to go to a web site in a range of situations, such as to complete a purchase. The FTC and others have emphasized the distinction between "first party" sites, the sites that a user decides to visit, and "third party" sites, which are the advertising networks, audience measurement firms, and others where the user did not deliberately choose to do business with the company.[69] The focus of much of the group's work has been on how to have effective user choice about tracking by third parties. There remain disagreements within the Working Group about where to draw the lines between first and third parties, and how parties in a first party setting at one time will operate in a third party setting at a later time. There has been consensus, however, that different overall rules apply to information gathered in a first party as contrasted with a third party setting.

The June Draft put forth a relatively broad definition of tracking with the rest of the specification defining permitted uses and thus narrowing the reach. The June Draft's

definition of tracking includes all online retention of data after displaying the web page: "*Tracking* is the retention or use, after a network interaction is complete, of data records that are, or can be, associated with a specific user, user agent, or device." Third parties "must not collect, retain, share, or use information related to the network interaction as part of which it received the DNT:1 signal outside of the permitted uses as defined within the standard and any explicitly granted exceptions." The definitions of collection, etc., state: "A party *collects* data if it receives the data and shares the data with other parties or stores the data for more than a transient period. A party *retains* data if data remains within a party's control beyond the scope of the current network interaction. A party *uses* data if the party processes the data for any purpose other than storage or merely forwarding it to another party. A party *shares* data if the party enables another party to receive or access that data."

C. The DAA Definition of "Tracking" and Related Terms

The DAA Proposal introduced a new definition of tracking: "Tracking is the collection and retention, or use of a user's browsing activity – the domains or URLs visited across non-affiliated websites -- linked to a specific user, computer, or device." Compliance for third parties omits the June Draft's text about "must not collect, retain, share, or use information." Instead, the DAA text states: "In a particular network interaction, if a third party receives a DNT: 1 signal, then that third party must not track outside of the Permitted Uses."

These definitions received extensive comments from those who objected to the DAA Proposal:

1. Justin Brookman of CDT, an editor for the compliance specification, described the DAA position: "Discussion on the mailing list and on calls indicates that its drafters believe the language would allow the use and retention of behavioral data for interest-based targeting, including retargeting. Moreover, industry would be able to retain for targeting (and any other) purpose any information about visited webpages, so long as the precise url from which it was derived was not discernible. Thus, companies could log precise descriptions of the content of every webpage visited if so desired, offering little to no incremental privacy protection, as it is the *content* of the webpages we view, not the technical web address, which is personal and sensitive."
2. Aleecia McDonald, of Stanford, and former co-chair of the Working Group, said that the discussion clarified that this proposal: "does allow companies to send a signal that they comply with DNT:1 while continuing to track, profile, and display targeted ads to DNT:1 users" and "places fewer restrictions than the DAA's existing opt-out program, which is already deemed too limited by regulators in the US and EU." She added: "We have had drafts on tracking for quite some time. While they did not entirely align, they were very far from this limited approach."
3. Jonathan Mayer, of Stanford, said that "data that is not considered "tracking" would be exempt from use limitations, collection minimization, retention transparency, and even reasonable security."

4. Chris Pedigo, of the Online Publishers Association, wrote: "We are concerned that this proposal would not meet with consumer expectations by allowing 3rd parties to continue serving behaviorally-targeted advertising to consumers who have activated DNT."
5. Mike O'Neill, of Baycloud Systems Limited, stated: "The main thrust of the DAA proposal is it allow companies to continue to build a permanent profile of everybody based on their web activity irrespective of the state of the DNT signal."
6. David Singer, of Apple, wrote: "Major change to the definition of tracking. I think that this new definition is not sufficiently tight, and is in a substantially different direction from the way we've been working."

The discussion here first addresses the narrow scope of the DAA Draft's definition of tracking. The DAA proposal only applies to specific URLs and excludes aggregate scoring (the common industry practice of assigning users to behavioral categories, such as "looking to buy a new car"). Second, this discussion addresses other objections to the DAA Draft's definition of tracking.

i. <u>The DAA Definition and Aggregate Scoring</u>

The DAA definition of tracking applies to "a user's browsing history, " which in turn means "the domains or URLs visited across non-affiliated websites." For this browsing history, the link must be cut to "a specific user, computer, or device." The DAA definition is narrower in various ways than the June Draft, which defines tracking as "the retention or use, after a network interaction is complete, of data records that are, or can be, associated with a specific user, user agent, or device."

One way that it is narrower, as discussed extensively in the group's teleconferences and emails, is that the DAA proposal does not apply to what DAA representatives call aggregate scoring. Aggregate scoring can exist whenever there has been deletion of "the domains or URLs visited across non-affiliated websites." Once the URLs are deleted, then a company can build a profile. The profile can: (1) indicate a user's interests; and (2) be linked to a unique identifier, such as a cookie. Advertisements can be served based on these profiles. In other words, aggregate scoring allows targeted online advertising for users who have turned on DNT:1.

Shane Wiley of Yahoo! wrote dozens of emails to the group explaining how this would work under the DAA Proposal. He wrote: "The clear issue is "indicative" versus "actual" browsing history. Actual browsing history would not be retained under Aggregate Scoring but does allow an aggregated summary of what may general indicate browsing history." He continued: "There could be multiple interest categories for a given user; for example, cookie ID 1234 could have an interest score of 4 in off-road vehicles and an interest score of 14 for flower purchase intender."

Aggregate scoring is permitted under the DAA Proposal because there is no "tracking" once the domains or URLs have been deleted. So long as those deletions happen, then targeted ads based on profiles are allowed whether or not DNT is turned on. As Shane

Wiley agreed on a teleconference, aggregate scoring is outside the scope of the Do Not Track standard.[70] As the discussion about aggregate scoring developed, Rob van Eijk, who represents the Article 29 Working Party of the European Union, wrote: "To me this reads as: aggregated scoring is out of scope for DNT. Not even a permitted use, but out of scope. This is a concern."[71] Other emails echoed these concerns.[72]

A different concern about aggregate scoring raised by commenters concerns reverse engineering or re-identification. Shane Wiley explained that the aggregate scoring exemption "would be similar to today's current interest-based advertising practices but will require some modification to ensure the result in all cases cannot be reverse engineered back to actual tracking details."[73] Detailed and credible technical criticisms on this issue came in emails from members of the Working Group, including Ed Felten (retargeting),[74] of Princeton and formerly at the FTC, Paul Ohm (k-anonymity),[75] at the University of Colorado and formerly at the FTC, and Justin Brookman of CDT (re-linking to URLs),[76] as well as a detailed comment written by Jonathan Mayer of Stanford (multiple technical issues).[77]

ii. Other Objections to the DAA Definition of Tracking

As shown above, the biggest theme in the comments criticizing the DAA definition of tracking is that it continues to allow online behavioral advertising, including for users who have turned on DNT:1. Other objections included:

1. Consumer confusion. The Online Publishing Association, John Simpson of Consumer Watchdog,[78] and others[79] stated that consumers would not reasonably be aware of what was meant by "Do Not Track" under the DAA definition of tracking. Within the Working Group, it took two teleconferences and many rounds of emails to develop a fairly clear idea of what the drafters intended with the definition. Typical users, in the view of multiple commenters, would not expect to continue to receive targeted online advertisements after choosing Do Not Track.
2. Charter. Aleecia McDonald of Stanford said: "My fundamental objection to this proposal is that it does not fulfill the TPWG Charter, which opens: '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.'" Her comments provide more detail about her concerns about charter violation.
3. Omission of network interaction language. David Singer explained that "removing "after the network transaction is complete" gives it a vague termination (as well as making it unclear to what extent our rules apply during the transaction)."[80] The comments note that, by removing that qualifier, the DAA Draft does not provide guidance on how long information may be retained before it falls within the definition of tracking.
4. Across non-affiliated websites. Under the DAA Draft, tracking only applies to "activities across non-affiliated websites." This would seem to exclude any restrictions on the common practice of retargeting (showing of advertisements

based on a user visiting only one website).[81] Rob van Eijk and Justin Brookman specifically mentioned allowing "retargeting" as a problem with the DAA Draft.[82]

5. Circumventing the group's work on permitted uses and other data controls. Jonathan Mayer of Stanford commented that a large portion of the group's work for the past two years has been on careful definition of permitted uses.[83] The implication is that much of the work on permitted uses would become irrelevant, because aggregate scoring and other data collection and use will fall out of scope. Minimization, security, and other protections will also no longer apply, because the activities will be out of scope.

In conclusion on Do Not Target, Justin Brookman summed up the history of the group on Do Not Target versus Do Not Target: "For years, the axes of this debate have been Do Not Collect versus Do Not Target, and over time and within the group, both sides had made meaningful concessions toward the other. At the very least, it was understood that DNT:1 would turn off ad targeting; the debate centered around what could be collected and retained for a narrow set of other permitted uses." The June Draft continues the longstanding understanding in the Working Group and the broader public that DNT:1 would turn off ad targeting, rather than having the user having to go to a separate self-regulatory program that is not based in the browser or other user agent. Based on the comments submitted by July 12, and the public record of the group, the June Draft matches the criteria of the Working Group on Do Not Target better than the DAA Proposal.

III. Do Not Collect

As documented in Part I of this Explanatory Memorandum, Do Not Collect has been a prominent theme in Do Not Track discussions since before the creation of the Working Group. Based on the comments received, and the previous public record, there is support for Do Not Collect from a range of participants, including at least consumer groups, Mozilla,[84] the Federal Trade Commission, and European regulators. The 2012 FTC Report, for instance, stated: "An effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (e.g., preventing click-fraud or collecting de-identified data for analytics purposes)."[85] Federal Trade Commissioner Julie Brill explained: "For me, one of the most critical points is that Do Not Track is not just Do Not Target ... but also, when the consumer so chooses, Do Not Collect."[86] Rob van Eijk, of the Article 29 Working Party in the EU, referring to European law requiring consent before data collection, stated that the DAA Proposal "does not provide the building blocks for consent that are required in the EU."[87] By contrast, advertising industry representatives have warned against Do Not Collect in the group, stressing how collection is needed to make the Internet operate properly, and that collection serves a range of valuable functions.

The discussion here focuses on transient or short-term collection, and then turns to the issue of unique identifiers.

A. Transient or Short-term Collection

Enabling transient or short-term collection has been a repeated response from group members to the concerns that collection is needed to make the Internet operate properly. The June Draft states that "a party *collects* data if it receives the data and shares the data with other parties or stores the data for more than a transient period." The mention of "more than a transient period" reflects widespread agreement in the group that some collection takes place during an initial period. There is a change proposal by Lee Tien of EFF and Jonathan Mayer of Stanford, two participants who have actively supported measures to reduce the use of unique identifiers. This change proposal states: "A third party may collect and use protocol information for any purpose, subject to a two-week retention period."[88] This proposal suggests that there may be a consensus for at least this sort of collection, although the group will need to go through the usual procedures to try to reach consensus on this issue. Previous discussions in the group have failed to reach consensus on the length of time that "short term" collection would be a permitted use. The record indicates, however, that under either base text the group would expect to have some provision for short-term collection, in order to ensure continued smooth operation of Internet activities.

B. Unique Identifiers

The June Draft tracking definition applies where data can be "associated with a specific user, user agent, or device." Without that association, no tracking occurs. Similarly, the June Draft says "a party collects data if it receives the data …" If a party never receives the data, then there is no collection.

The unique identifier issue has been debated extensively in the group, including at the Sunnyvale face-to-face. That meeting concluded with the Consensus Action Summary, which stated: "There will be ongoing discussions of unique identifiers as a critical issue for advocates. We are inviting proposals on ways to solve this issue going forward."[89] During that meeting, a number of participants indicated that they would strongly object to any standard that did not address unique identifiers.

The Electronic Frontier Foundation provides the most detailed comment about unique identifiers:

> "Unique identifiers
>
> Removing the text on unique identifiers means that the DAA text does not require that DNT mean "Do Not Collect". But for sufficient privacy protections to exist for consumers, DNT must ensure that tracking information about individuals is not collected. While in an ideal world, the privacy policies of companies would be detailed and short and hard limits on data retention could be relied upon, there are many reasons why practically speaking we must insist on a Do Not Collect. First, companies do not have policies with short and hard limits on data retention. Second, even if strong retention limits were in place, we have seen that other actors like

governments regularly have access to this data via legal process. Third, de-identification is an evolving field, and until users have more confidence that their data is being aggregated responsibly, these users have the right to opt out of collection altogether. Fourth, the policies of companies change, and there is no substitute for knowing in a reliable and auditable way that information is simply not being collected.

It has been a central tenet of EFF that DNT must curb collection. In particular, a user who indicates that she does not want to be tracked by third parties should not have a unique id assigned to her, her user agent or device, that would allow her records to be linked together. Industry claims of the impossibility of this are far overblown. Large industry players regularly forgo the use of unique id tracking cookies, and cookies are regularly blocked in the ordinary course of Internet usage for reasons related to privacy and security. The web doesn't break as a result for users who block cookies, or for companies who do not set them in every circumstance."[90]

The unique identifier issue has been linked in the group's discussions with the issue of permitted uses. The idea of permitted uses has been that they are uses necessary for the functioning of the web, such as security and de-bugging, and are allowed even when a user has turned on DNT:1. The June Draft contains a number of these permitted uses. On the other hand, consumer groups and others have maintained that the use of unique identifiers even for some or all of these permitted uses is collection of data contrary to the purpose of DNT, and that other technologies are available to achieve the industry's needs.[91]

The June Draft has two provisions concerning unique identifiers. The first permits the use of unique identifiers only for permitted uses: "A third party that does not require unique user identifiers for one of the permitted uses must not place a unique identifier in cookies or other browser-based local storage mechanisms." This is a minimization requirement – third parties may use unique identifiers where necessary for the permitted use, but not beyond that.

The second provision in the June Draft limits the use of unique identifiers if other technologies become reasonably available: "Third Parties must make reasonable data minimization efforts to ensure that only the data necessary for the permitted use is retained, and must not rely on unique identifiers for users or devices if alternative solutions are reasonably available." Except for proposed deletion of this provision in the DAA Proposal, the only change proposal for this text came from Amy Colando of Microsoft, who would add "and technically feasible" to the end of the sentence.

In response to the June Draft, Mike Zaneis of IAB said: "We don't know what's 'reasonably available.' Cookies have been the building block for a long time. We don't have a sense of what people want or mean, so we couldn't commit to a theoretical mechanism. We don't understand what's being asked of us."[92] Concerns about over- and under-specificity have come up in the group on numerous other issues, including de-identification, transient, and others. One way to address such concerns is to use non-

normative text to provide commentary on what a term means.

The other comment by July 12 that addressed unique identifiers explicitly was from Shane Wiley of Yahoo! He wrote: "Unique IDs, their setting, collection, and utility is one such topic that is best reserved for a different discussion such that HTML cookies, LSOs such as Flash Cookies and HTML 5 Persistent Stores, Browser Fingerprints, and future possible innovations in online IDs can be appropriately addressed in their entirety. The DAA Proposal appropriately removes this element to create a better starting point to focus our efforts."[93] Relevant to that comment may be two items: (1) as discussed in the history section, the issue of persistent or unique identifiers has been part of Do Not Track efforts since before the creation of the Working Group; and (2) a theme of Do Not Track work has been to seek technology-neutral approaches.

One other advertising industry comment stated that "customization is not necessarily privacy-intrusive." David Wainberg of AppNexus wrote: "Proposals, such as the low-entropy cookie idea from the EFF or the alternative browsing history/de-identification approach, demonstrate that customization is not necessarily privacy-intrusive, and that it may be possible to have a balanced and tailored approach that advances privacy while preserving competition and gaining a high rate of adoption."[94] Based on discussions in the group, an industry approach that overlapped with the 2012 EFF/Mozilla/Stanford proposal about low-entropy cookies would appear to have the potential to gain support from diverse stakeholders.

Two other comments criticized the lack of explanation, in connection with the DAA Proposal, about why the provisions about unique identifiers were deleted. John Simpson said that the removal of this provision "removes a modest privacy friendly requirement without justification or explanation."[95] Jonathan Mayer said: "The DAA proposal omits any reference to privacy-preserving technologies. Where an alternative to present practices is available and accommodates consumer privacy concerns, why would we not encourage this win-win?"[96]

In conclusion on Do Not Collect, the consistent position of a number of stakeholders has been that addressing unique identifiers is a sine qua non for their agreeing to a standard. The current cookie-based ecosystem is relatively new; as recently as 2003 the main third-party advertising organization had only two members.[97] As industry representatives have stressed in the group, advertising practices evolve quickly. The June Draft leaves open the possibility that a next-generation ecosystem can develop with effective advertising as well as user privacy and choice, while the DAA Proposal assumes that the highly identified methods of the status quo are all that should be expected. In order to create the possibility of a consensus that includes consumer groups, and is based on the history and the group charter's mention of "blocking or allowing Web tracking elements," the June Draft better reflects the views of the Working Group on Do Not Collect than the DAA Proposal.

Part IV: Data Hygiene and De-Identification

In the group's discussions, the term "data hygiene" refers to a range of controls that a company may apply to de-identify data and reduce the risk that data is revealed without authorization. Information about users is collected for a variety of legitimate reasons; once that data is collected, however, a broad range of stakeholders agrees that the holders of data should exercise good hygiene, preventing data spills and generally treating users' data securely and appropriately.

The topic of de-identification has been a major focus of the group's work in 2013. An important reason for this focus has been a consensus in the group that data at some point is scrubbed enough so that data becomes out of scope of the DNT specification. Put another way, data at some point is de-linked or de-identified enough that use of it does not count as "tracking." In drawing the line between in-scope and out-of-scope, a major privacy concern is that data might be re-identified. Therefore, more scrubbing creates less risk for individuals. A major industry concern has been to retain the utility of data, and more scrubbing often means lower usefulness for industry.

The June Draft treatment of de-identification is quite similar to wording in the 2012 FTC report. "Data is *deidentified* when a party: (1) has achieved a reasonable level of justified confidence that the data cannot be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device; (2) commits to try not to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." A number of change proposals have been submitted on this issue, and those non-DAA change proposals will be before the group as we continue our work.

The DAA Proposal calls for a combination of technical, administrative, and operational controls to move tracking data as originally collected ("raw" or "red" data) to what it calls a de-identified state ("yellow" data). It then defines additional technical measures that would move the data to a de-linked state ("green" data).

It has been difficult to reach consensus on de-identification because of contrary but strongly-held views by professionals in the field. As Dan Auerbach of EFF notes: "We simply do not agree about what properties a data set must have before it is considered de-identified and hence out of scope for DNT."[98] Notably, there has been a longstanding disagreement in the group about the extent to which non-technical controls are sufficient to have a data set qualify as de-identified.[99] Shane Wiley of Yahoo! has provided the most detailed presentations to the group about the usefulness of such administrative and operational controls, while participants including Dan Auerbach of EFF, Ed Felten of Princeton, Aleecia MacDonald of Stanford, Jonathan Mayer of Stanford, Mike O'Neill of Baycloud Systems Limited, and Rob van Eijk of the Article 29 Working Party have often disagreed with Shane Wiley on the subject.

Rather than seeking to announce some categorical judgment on the relative usefulness of administrative and operational controls, the basis for the group decision on data hygiene arises from a number of other factors:

1. Lack of clear match between proposed text and working example of de-identification. Shane Wiley has provided considerable detail to the group about one implementation of the DAA data hygiene proposal.[100] EFF's comment and extensive discussion on the email list showed a number of respects where the submitted text of the DAA proposal did not appear to match the implementation example.
2. Narrow scope of what is covered by the data hygiene proposal. As discussed in Part II, de-identification applies only to "tracking" data as defined in the DAA Proposal, notably including the domains or URLs that an individual or device has visited with a browser. Part II discussed the topic of aggregate scoring in detail, including the range of credible technical arguments that members of the group have raised about ways data outside of that tracking definition can be re-identified.
3. Credible ways to re-identify data. Jonathan Mayer made the most detailed comments on ways to re-identify data that is considered de-identified under the DAA Proposal.[101] Aleecia MacDonald[102] and Mike O'Neill[103] made similar points about the ability to re-identify a hashed URL.
4. Lack of Answers to Important Threat Models. Justin Brookman of CDT examined the protections offered by the DAA Proposal and concluded: "This model does not provide complete protection to the threat of data breach or internal misuse, or much protection at all to compelled disclosure pursuant to a subpoena or law enforcement request."[104]
5. Use of the Term "De-Identification." Although the question of terminology may seem a relatively minor matter, the group has spent significant time discussing the DAA Proposal's use of the term de-identification for the yellow state, including multiple action items assigned to try to resolve terminology.[105] The DAA Proposal, apparently consistent with the term's use in the DAA's self-regulatory code, uses the term "de-identified" at a stage where a company retains the information needed to re-identify an individual. This threshold for "de-identification" is less strict than usage of the term in other privacy regimes, such as the U.S. medical privacy rule or the European Union.
6. Data hygiene should apply in general, and not just to DNT:1 users. Justin Brookman of CDT made the point that "companies should adopt strong data hygiene practices for *all* users."[106] There were no comments explaining why data hygiene should not apply generally.

For these reasons, the DAA Proposal on de-identification, taken together with its novel definition of tracking, does not reflect the views of the Working Group as well as the June Draft, as a basis for moving forward on data hygiene and de-identification issues.

A. Market Research and Product Development Exceptions

The chairs recognize the considerable work that members of the DAA have devoted to crafting data hygiene proposals. Indeed, the DAA Proposal includes new details for how DAA members could address the market research and product development exceptions to the current DAA Principles. The data hygiene proposals state that market research and product development would occur in the intermediate "yellow" state. In contrast, the

current DAA Principles permit those activities to use raw or "red" data. In this way, the DAA could consider changing its own self-regulatory program to fulfill its previous statements that it would tighten its market research and product development exceptions.[107]

This improvement in treatment of those exceptions, however, does not constitute a general regime that consumers would reasonably expect to be included in the scope of Do Not Track. The comments support the conclusion that the June Draft provides a better platform for building an overall approach to data hygiene and de-identification.

V: **Responses to Comments That Support the DAA Proposal as Base Text**

By the July 12 deadline, there were 27 comments submitted in the formal call for objections, as well as hundreds of emails on the group's public mailing list in recent weeks. This memorandum was drafted after review of all of these comments and emails. This section responds to five themes in comments that favored adopting the DAA Proposals as the base text: adoption and significant change from the status quo; balancing privacy vs. the web ecosystem; proliferation of DNT:1 signals; competition concerns; and three-state approach to de-identification.

A. Adoption and Significant Change from the Status Quo

Several working group members mentioned the high level of adoption by industry participants if the DAA Draft is selected as the base text, contrasted with what they expect to be low adoption if the June Draft is selected as the base text.[108] In the Boston face-to-face meeting, adoption was stated as one of the five criteria for a successful standard. From the initial discussion of the criteria in Boston, however, the group understood that the criterion of adoption was in potential conflict with the criterion of a significant change from the status quo. Mike O'Neill of Baycloud Systems Limited referred to this discussion in commenting about the DAA Proposal: "If this proposal is used as a basis we would have the 'null' standard Peter warned us about" at the Boston face-to-face.[109]

In terms of adoption, comments from browser companies Apple, Microsoft, and Mozilla all supported using the June Draft as base text rather than the DAA Proposal. Browser companies Google and Opera did not submit comments for July 12, but both have been implementing DNT into their browsers. These user agents are important to assessing the level of adoption of a DNT standard,

Comments from the group differ considerably about the extent to which the DAA Proposal varies from the status quo. As discussed in Part IV, the data hygiene provisions are departures from the status quo compared with the DAA's existing self-regulatory principles. Representatives of the DAA have previously and publicly committed to addressing criticisms of the market research and product development exceptions to their existing principles.[110] Part IV discussed that the data hygiene provisions specifically address conducting market research and product development in the yellow state, while the current version of the DAA principles permit those to be conducted in the red state. The data hygiene provisions thus can be understood as measures designed to fix

acknowledged problems with the DAA principles. As in discussions of the Draft Framework, it may be that these portions of the DAA Proposal would be supported as part of an overall package but not in isolation. That is a decision for the DAA to make within its self-regulatory principles.

Concerning overall change from the status quo, the decision on which base text to use described the data hygiene proposals and concluded: "By themselves, however, they do not address the 'tracking' in Do Not Track." The DAA Proposal does not use the DNT signal to trigger any change in Do Not Target or Do Not Collect, and so is not a significant enough change in the status quo to meet the criteria of the group.

B. Balancing privacy vs. the web ecosystem

Lou Mastria of the DAA and other Working Group members commented that the DAA Draft, in contrast to the June Draft, strikes a better balance of how to protect privacy interests while maintaining the existing web ecosystem.[111] David Wainberg explained the perceived misbalance in the June Draft: "The approach in the June Draft, because it is not tailored to a specific problem, is over-broad such that, if implemented, it would be harmful to the diversity of content producers on the Internet today, and would not provide a commensurate net privacy benefit to consumers."[112]

Based on the overall discussions in the Working Group in the past two years, participants vary widely in how they perceive the best balance between privacy and user choice, on the one hand, and harms to the existing web ecosystem, on the other. Based on these discussions, participants also vary in whether they believe that this "balancing" approach is a useful way to understand the problems facing the group. Some participants, for instance, have stated that the web ecosystem will be better in multiple respects, including economic growth, if privacy and user choice are well protected in a Do Not Track standard.

Based on discussions in the group, one reason to draft a DNT standard broader than the DAA Proposals is to take advantage of the opportunity presented by the Tracking Protection Working Group. For two years, experts from numerous parts of the Internet ecosystem have worked hard to tailor a standard that addresses the multiple goals that exist for such a complex global ecosystem. The comments filed by July 12 indicate the intelligence, expertise, and diversity of perspective of members of this group. The public attention to the group's work, including by governmental leaders, is an indication of the opportunity that many see for what can emerge from the group's efforts.

Discussions in the group indicate a wide range of views on whether and to what extent a DNT standard would harm the economics of the web. The behavioral advertising ecosystem under discussion in the Working Group is quite recent. The NAI, for instance, was down to fewer than 5 members in 2004 and is now approaching 100 members.[113] Given that business models have evolved quite rapidly and recently, there is limited reason to believe the status quo of 2013 is either enduring or the best achievable approach for the web ecosystem. Indeed, one reason for the June Draft's provisions on unique identifiers is

to leave the web open to innovation that can achieve effective advertising and monetization while also better achieving user privacy and choice.

One reason to doubt the persistence of today's status quo is the arms race often discussed within the Working Group. As the group has discussed, that arms race has in some respects already begun: "The digital cookies currently used to track user habits are blocked by the browsers — only to have the advertisers respond with even more sophisticated tracking methods like digital fingerprinting.[114] The group has often discussed how lack of agreement could cause more harm to the ecosystem, in the form of the arms race, than a negotiated standard that incorporates insights from diverse stakeholder perspectives.

C. Proliferation of DNT:1 Signals

Comments favoring the DAA Draft expressed concern about the proliferation of DNT:1 signals.[115] Mike Zaneis of the IAB, in explaining the DAA Proposal during a teleconference, explained the concern: "My members are now seeing 20-25% of user base sending DNT flag. Early on, our position had been: perhaps the W3C could standardize the DNT signal, and we would treat that as an industry opt-out. That is no longer tenable. We expect DNT:1 signals to approach 50% in the short-term."[116] He said that, instead of providing an industry opt-out, the DAA Proposal is "[m]ore of a data hygiene practice."

Shane Wiley made a similar point in terms of the technical ease of sending DNT:1 signals: "The ease at which injecting the DNT:1 signal in headers (Mozilla states it took only 13 lines of code), the lack of technical mechanisms to ensure this only occurs by user action, and the proliferation of signals coming from browser add-ons, privacy tools, anti-virus applications, network intermediaries such as WiFi access points and routers, and others, leads many technical experts on all sides of the table (consumer advocate, browser vendor, and industry) to predict DNT:1 rates above 50% - possibly even above 80%."[117] Members of the group have said that a particular rate of DNT:1 should not be a basis for what the standard says, if the rate reflects actual choice by the user. DAA members and others have expressed particular concern, however, about being expected to comply with DNT signals that are not set by the user.

The full extent of this problem is not clear. Alex Fowler from Mozilla called for evidence of DNT signals reaching above 50%: "Apologies if this has been documented somewhere in our discussions and I missed it, but I'm seeing more and more claims of the proliferation of DNT:1 online, especially outside the browser context. Can someone point me to a published study or paper that makes this clear and the sources for these signals? For my part, I'm looking into the extent to which DNT may or may not be sent today by specific Firefox add-ons. If we're going to consider this as a factor for which signals are OK and also as a justification for which path we follow, it would be helpful for the basis for this claim to be incontrovertible."[118]

Despite the lack of consensus about the facts on this issue, the June Draft contains provisions designed to ensure that DNT signals reflect actual user choice. There are currently change proposals dealing with user agents and what constitutes user choice in

the compliance specification, as well as provisions in the TPE specification. It is also worth noting that the DAA Draft does not differ from the June Draft on text designed to address the potential problem of DNT proliferation.

D. Competition Concerns

Members of the Working Group, most notably Alan Chapell, have commented that the provisions concerning first and third parties will favor large first parties in ways that harm competition.[119] A number of change proposals are before the Working Group concerning the treatment of first parties vis-à-vis third parties, and W3C staff has worked with stakeholders recently on this topic in an effort to find consensus. The choice of base text does not preclude full discussion of competition and other considerations as the group considers these change proposals.

E. Three-state approach to de-identification

Members of the Working Group commented in favor of the three-state approach to de-identification compared to the two-state de-identification approach in the June Draft.[120] The group decision does not take a position on whether to use a two- or three-state de-identification process. The DAA Draft includes language on de-identification language is not adopted as the base for the working group. The three-state de-identification process proposed by Rob van Eijk, however, is not blocked by this chairs' decision,[121] and Dan Auerbach, who has favored a two-stage approach to de-identification, has written that the number of stages is not as important in his view as the nature of the protections.[122]

VI. Conclusion

As shown in the history section of this document, the issues that separate theJune Draft and the DAA Proposal have been the subject of extensive discussion in the Working Group throughout 2013. The decision of the Working Group, and this memorandum, is based on the comments submitted by July 12, as well as the emails and other public records established for the Working Group. ISSUE 215, the choice of base text, is hereby closed, and the June Draft will be the base text for the group's continued work. As previously noted, this decision also substantially affects ISSUE 5 (tracking), 16 (definition of collection, etc.), 188 (unique identifiers), and 191 (de-identification). Having considered the points above, we will not accept change proposals that are merely re-statements of these elements from the DAA proposal.

The Working Group will turn to examination of the other change proposals to theJune Draft, as announced previously to the group and as listed on the group's web page. We plan to work on these immediately in the weekly call on July 17, and will seek to close as many as possible this month. Before the end of July, the group will discuss whether and how to proceed in light of the current Last Call deadline scheduled for the end of July.

[1] Note on references: citations to the comments on the Call for Objections page are listed as "CFO." These comments can be found at http://www.w3.org/2002/09/wbs/49311/datahygiene/results.

[2] Shortly before this document was posted, on July 16, Stu Ingis of the DAA emailed Swire to say that the DAA was one of many groups that supported the proposed alternative base text, and it should not be called the "DAA Proposal." The July 15 opinion referred to this approach as the "DAA Proposal," and this Explanatory Memorandum, to be consistent, does the same. The approach was referred to in that way in group teleconferences during the past two weeks, and on the website in the formal call for objections. Lou Mastria of the DAA, in his comments, wrote: "One ministerial clarification…while Option A has come to be called the DAA Proposal, it is important to note that this consensus approach was developed and submitted by a an entire cross-section of responsible industry entities who all seek to provide a pragmatic way forward that achieves real privacy protections while continuing to support the ad-funded Internet we've all come to love." CFO, Lou Mastria, DAA. This comment was the only indication received by W3C before July 16 of concern about the name for the proposal as posted on the W3C web site.

[3] The W3C thanks Yianni Lagos for his assistance in preparation of this Explanatory Memorandum.

[4] CONSUMER RIGHTS AND PROTECTIONS IN THE BEHAVIORAL ADVERTISING SECTOR, http://www.ftc.gov/os/comments/behavioraladvertising/071115jointconsensus.pdf.

[5] FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[6] Neelie Kroes, *Why we need a sound Do-Not-Track standard for privacy online*, Blog of Neelie Kroes, Vince President of the European Commission (2012), http://blogs.ec.europa.eu/neelie-kroes/donottrack/.

[7] DAA POSITION ON BROWSER BASED CHOICE MECHANISM, https://www.aboutads.info/resource/download/DAA_Commitment.pdf.

[8] PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, FTC REPORT, http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[9] KHALED EL EMAM, GUIDE TO THE DE-IDENTIFICATION OF PERSONAL HEALTH INFORMATION (2013).

[10] Opening Plenary Cambridge F2F, slide 6, http://www.w3.org/2011/tracking-protection/mit/plenary.swire.021113.pptx.pdf.
[11] Tracking Protection Working Group Charter, http://www.w3.org/2011/tracking-protection/charter.
[12] Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).
[13] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005).
[14] Chris Mejia, "When talking about security we use every means available. We would be taking a step back if we did not use cookies. We have a fiduciary responsibility to protect our uses, part of that is using the information that we gather to protect them." http://www.w3.org/2013/05/07-dnt-minutes (slight corrections to minutes are made throughout this memorandum to fix typos)
[15] At the Sunnyvale Face-to-Face, we had a session on this topic with invited guest speaker Jon Callas, a cybersecurity expert. Callas concluded that there may be a small harm to security if the detailed records are not retained, but said he believed that the privacy gains were greater: "want to make a privacy friendly system, and one that is good for security. Does it justify tagging everyone? For security purposes, you could do something else that is as or more effective. If you saw something that was security related, you set on an alarm; I have far less problem with tagging." http://www.w3.org/2013/05/07-dnt-minutes. The group did not reach consensus about the need for long-term storage of detailed URIs for security purposes.
[16] Peter Swire said: "Mayer discussed the marginal value of unique ID cookies. Shane explained [without the use of cookies] the loss of identifying bad actors at the beginning of an attack and the inability to set a honeypot [a trap to detect and catch a computer hacker]. Response back [from Jon Callas] was that privacy implications were greater [than the security implications]. We did clarify what is in and out of [the security] discussion. I have not heard why the things Shane said were de minimis. We clarified issues; I will consider this part of the discussion closed." http://www.w3.org/2013/05/07-dnt-minutes#item01.
[17] George Ivie said: "Some companies say they cannot retain data for privacy purposes. . . . If company says we cannot retain it at all, MRC says you do not have to retain if they have a legitimate reason" http://www.w3.org/2013/02/06-dnt-minutes.
[18] http://lists.w3.org/Archives/Public/public-tracking/2012Jul/0184.html.
[19] Rena Mears "pcob says 7 years" http://www.w3.org/2013/03/27-dnt-minutes.
[20] Justin Brookman wrote: "But it doesn't sound like you're required to retain that for seven years -- speakers just said that companies often aggregate at some point." Shane Wiley wrote: "Justin, agreed - at some point aggregation is acceptable - question is when. Some argue a few years - some argue something longer. It's a corporate risk dimension - what level of financial risk do you take on by aggregating data too soon?" "Dan Auerbach said: "If I am an ad network that wants to delete raw log data after 2 months, Rena Mears urged caution. Might that change?" http://www.w3.org/2013/03/27-dnt-minutes.
[21] *Id.*
[22] http://lists.w3.org/Archives/Public/public-tracking/2012Feb/0049.html
[23] *Id.*

[24] Do Not Track – Compromise Proposal, http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0095/compromise-proposal-pde-tl-jm.pdf.
[25] David Wainberg stated: "when we talk about minimizing URIs, buckets, these are on the targeting side." http://www.w3.org/2013/02/11-dnt-minutes.
[26] Shane Wiley wrote: "Actual site activity details will be aggregated away such that only the ID and the aggregate score remain. This would be similar to today's current interest-based advertising practices but will require some modification to ensure the result in all cases cannot be reverse engineered back to actual tracking details. Of course this would still be able to be turned off via industry opt-out pages, AdChoices icon, 3rd party tools, etc. More than a single interest score is expected to exist for a single cookie. For example, cookie ID 1234 has an interest score of 4 for off-road vehicles and an interest score of 12 for flower purchase intent." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0320.html
[27] *See* Do Not Track – Compromise Proposal, http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0095/compromise-proposal-pde-tl-jm.pdf.
[28] Shane Wiley wrote: "This would be similar to today's current interest-based advertising practices but will require some modification to ensure the result in all cases cannot be reverse engineered back to actual tracking details." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0320.html. Mike Zaneis suggested that the standard is not "do not collect." http://www.c-spanvideo.org/program/DoNotT.
[29] FTC explained the need for a do not collect standard: "an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (e.g., preventing click-fraud or collecting de-identified data for analytics purposes)." PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, FTC STAFF REPORT, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; Federal Trade Commissioner Julie Brill explained: "For me, one of the most critical points is that Do Not Track is not just Do Not Target ... but also, when the consumer so chooses, Do Not Collect." Wendy Davis, *FTC's Brill: 'Do Not Track' Means Do Not Collect Data* (Mar 2, 2012), http://www.mediapost.com/publications/article/169317/ftcs-brill-do-not-track-means-do-not-collect-d.html#ixzz2Ym0RSXK8. Dan Auerbach wrote: "It has been a central tenet of EFF that DNT must curb collection. Call For Objections (CFO), Dan Auerbach, EFF. Ed Felten wanted to confirm: "can a DAA representative confirm that the current DAA framework limits collection?" http://www.w3.org/2013/05/01-dnt-minutes.
[30] Jonathan Mayer wrote: "I would encourage participants following this topic to read a blog post on privacy-improved advertising measurement that I co-authored with Arvind Narayanan." http://lists.w3.org/Archives/Public/public-tracking/2012Jul/0124.html.
[31] "We don't know what's 'reasonably available.' Cookies have been the building block for a long time. We don't have a sense of what people want or mean, so we couldn't commit to a theoretical mechanism. We don't understand what's being asked of us." http://www.w3.org/2013/07/03-dnt-minutes.

[32] Draft Framework for DNT Discussions Leading Up to Face-to-Face, http://lists.w3.org/Archives/Public/public-tracking/2013Apr/att-0298/one_pager_framework_as_distributed.pdf.
[33] *Id.* part 6.
[34] Consensus Action Summary, http://op.bna.com/der.nsf/id/sbay-97jv8n/$File/aa130509-2.pdf.
[35] http://www.w3.org/2013/04/29-dnt-minutes.
[36] Peter Swire stated: "Where did draft framework come from? From you, might sound silly, but much of the material came after discussions between folks, including browsers and advertisers. There have been discussions between browsers and consumer groups. There have been blogs, discussions, lots of discussions I have not been in room for including between advertisers and consumer groups. Most of the words in the Framework did not come from me, and I was not even in room. [The Framework] represents different stakeholders, and regulators have weighed in. Lots of people [have been] talking to each other." http://www.w3.org/2013/05/01-dnt-minutes.
[37] Peter Swire stated: "Draft framework is a DRAFT and a FRAMEWORK....not a secret deal, but helps with the agenda for the meeting." http://www.w3.org/2013/05/01-dnt-minutes.
[38] Ed Felten discussion of user agents found at http://lists.w3.org/Archives/Public/public-tracking/2013Apr/0136.html.
[39] Shane Wiley wrote: "The ease at which injecting the DNT:1 signal in headers (Mozilla states it took only 13 lines of code), the lack of technical mechanisms to ensure this only occurs by user action, and the proliferation of signals coming from browser add-ons, privacy tools, anti-virus applications, network intermediaries such as WiFi access points and routers, and others, leads many technical experts on all sides of the table (consumer advocate, browser vendor, and industry) to predict DNT:1 rates above 50% - possibly even above 80%." CFO, Shane Wiley, Yahoo!.
[40] Draft Framework for DNT Discussions Leading up to Face-to-Face, http://lists.w3.org/Archives/Public/public-tracking/2013Apr/att-0298/one_pager_framework_as_distributed.pdf. Discussion of user agent requirements at Sunnyvale found at http://www.w3.org/2013/05/08-dnt-minutes#item03.
[41] http://www.w3.org/2013/07/03-dnt-minutes.
[42] http://www.w3.org/2013/07/03-dnt-minutes.
[43] CFO, Shane Wiley, Yahoo!.
[44] Tracking Compliance and Scope – June Draft, http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance-june.html.
[45] Tracking Compliance and Scope – W3C Working Draft 30 April 2013, http://www.w3.org/TR/tracking-compliance/.
[46] http://lists.w3.org/Archives/Public/public-tracking/2013Jun/0031.html.
[47] http://lists.w3.org/Archives/Public/public-tracking/2013Jun/0220.html.
[48] http://lists.w3.org/Archives/Public/public-tracking/2013Jun/0397.html.
[49] http://www.w3.org/2013/06/26-dnt-minutes.
[50] http://lists.w3.org/Archives/Public/public-tracking/2013Jun/0518.html.
[51] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0020.html.
[52] http://lists.w3.org/Archives/Public/public-tracking/2012Sep/0197.html.
[53] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0076.html.

[54] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0140.html.
[55] Sarah Branham, *What Do We Really Mean When We Say We Will Not Track* http://adage.com/article/guest-columnists/track-online/234559/.
[56] Tony Romm, *What exactly does 'do not track' mean?*, Politico, http://www.politico.com/news/stories/0312/73976_Page3.html.
[57] http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.
[58] http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.
[59] http://www.youradchoices.com/faq.aspx.
[60] Testimony of Lou Mastria, Managing Director of Digital Advertising Association (April 24, 2013), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=cd2e39e0-6825-4b8c-9789-40d26a72d457.
[61] *Id.*
[62] Statement of Justin Brookman, Director, Consumer Privacy Center of Center for Democracy and Technology, https://www.cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.
[63] Testimony of Lou Mastria, Managing Director of Digital Advertising Association (April 24, 2013).
[64] A USA Today/Gallup poll found that 67% of internet users believe that advertisers should not track users online. Lymari Morales, *U.S. Internet Users Ready to Limit Online Tracking for Ads* (2010), http://www.gallup.com/poll/145337/Internet-Users-Ready-Limit-Online-Tracking-Ads.aspx. The 1% rate is also lower than user preferences indicated by a Zogby Analytics poll commissioned by the DAA. That poll reported that 22% of users favored a law restricting internet advertising and 4% of users found behaviorally targeted internet advertising their single biggest concern on the internet, more concerning than identity theft and computer viruses. Interactive Survey of US Adults (2013), http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf.
[65] "Many users visit the website, learn about their choices, and ultimately choose not to opt out. We believe that this shows that once consumers understand how online advertising works, many prefer to receive relevant ads over irrelevant ads." Testimony of Lou Mastria, Managing Director of Digital Advertising Association (April 24, 2013).
[66] https://www.aboutads.info/resource/download/DAA_Commitment.pdf.
[67] http://ftc.gov/os/2012/03/120326privacyreport.pdf.
[68] Draft Framework for DNT Discussions Leading Up to Face-to-Face, htttp://lists.w3.org/Archives/Public/public-tracking/2013Apr/att 0298/one_pager_framework_as_distributed.pdf.
[69] The 2009 FTC Staff Report stated: "staff agrees that "first party" behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites." http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf, at p. 26.
[70] Justin Brookman asked: "Though, to be clear, derived info from urls is completely out of scope too." Shane Wiley responded: "Justin - correct - as long as they cannot be reversed back to "tracking" data, they are outside of scope since they are "not tracking"". http://www.w3.org/2013/07/10-dnt-minutes.

[71] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0262.html.
[7272] Mike O'Neil, from Baycloud Systems Limited, explained the problem with the DAA Draft approach: "There is not much difference between the retention of a profile based on algorithmically examining a web history and the actual web history itself. Both can be a basis for discrimination." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0240.html; Lauren Gelman, from Blurry Edge Strategies, explained how the aggregate scoring exemption may engulf the rule: "If collection is permitted in order to allow the business to translate the URL into a segment, the exception has indeed, finally, swallowed the rule." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0309.html .
[73] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0320.html.
[74] Let me add some detail to Jules's retargeting example. Suppose I visit examplestore.com and look at surfboards, but don't buy anything. Later when I'm reading the unaffiliated site localnewspaper.com, an ad pops up for ExampleStore brand surfboards. This happened because examplestore.com put a unique ID cookie on my computer when I visited the store, then used its third-party presence on the localnewspaper.com site to notice my unique ID cookie and connect it to my previous surfboard shopping. Is this allowed under the DAA proposal, for a DNT:1 user?
[75] Paul Ohm wrote: "Would it be considered tracking if a particular cookie was scored high in the category, "visited one of these two particular URLs," because it could not possibly be reverse engineered to a single URL?
And if "visited one of these two particular URLs" is some how considered tracking, what in any of the various draft spec texts leads us to that conclusion?
And if "visited one of these two particular URLs" is considered tracking, what about "visited one of these ten particular URLs"? Or "visited one of these 100 particular URLs"?
In other words, is there a k-anonymity floor operating here? If so, what is k?"
http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0333.html.
[76] Shane Wiley described, "The goal is to ensure the isolated aggregate score cannot be reverse engineered to the actual activity (URL is used as the primary example of activity but as we discussed yesterday there are other valid activities that could occur that would be caught by this term) of the user. If a website were to create two URLs to the exact same page as a way to somehow argue this provided an "aggregate" view, I believe they would NOT be in compliance and would indeed be "Tracking"."
http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0351.html . Justin Brookman responded: "It is not at all clear how closely related the attributes can be to the content of the webpage. I just looked at the Braves box score from yesterday (they lost) --- what attribute scoring can come out of that that isn't "browsing activity --- the domains or urls visited across non-affiliated websites"? "ESPN.com/12345" is out. But what about "Braves-Marlins box score, 7/10/13"? "Braves box score"? "Braves"? "Baseball"? "Sports?" Are you saying the line should be between "Braves box score" and "Braves"? In any event, the text as drafted is not helpful in making that distinction, and so it's hard to see this as a robust privacy-preserving mechanism. But if you're intending it as such, that would be good to know." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0354.html.
[77] CFO, Jonathan Mayer, Stanford University.

[78] CFO, John Simpson, Consumer Watchdog: "As has become clear in repeated email chains this week and on our conference call, the text does not clearly, concisely and accurately reflect to the average reader what in many cases the proposers say is their intent."
[79] CFO, Justin Brookman, CDT: "Allowing behavioral targeting and retargeting would run strongly counter to a consumer's reasonable expectations in turning on Do Not Track, and this standard should not allow it."
[80] CFO, David Singer, Apple.
[81] Shane Wiley explained: "Retargeting is a function of a Service Provider – not expressly cross-site activity as in behavioral advertising – in this context." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0339.html. The language proposed in the DAA Draft matches closely with the DAA's Online Behavioral Advertising Principles. In the ruling by the Council of Better Business Bureaus in Microsoft Advertising, Case Number: 17-2012, a form of retargeting was found to be outside the scope of the OBA Principles. http://www.bbb.org/us/storage/113/documents/online-behavioral-advertising/Microsoft%20Atlas%20Decision%20For%20Release.pdf.
[82] CFO, Rob van Eijk, Article 29 Data Protection Working Party; CFO, Justin Brookman, CDT.
[83] "I'm greatly concerned about overloading the term 'tracking' with substantial and non-obvious consequences, such as exempting present behavioral advertising practices. That's certainly not clear from the text, nor does it accord with our past practice of identifying individual permitted uses (including where non-URL data is involved)." http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0310.html.
[84] CFO, Sid Stamm, Mozilla: "Many people are activating DNT because they want unauthorized data collection and tracking to stop. Making a weaker standard where collection continues as-is and compliant service providers only claim to use the data for fewer things would clearly be ignoring these widespread pleas."
[85] http://www.ftc.gov/os/2012/03/120326privacyreport.pdf . Chairman Leibowitz similarly stated that "the commission took DNT to mean not collecting any data from customers." http://www.nytimes.com/2012/03/30/technology/debating-the-path-to-do-not-track.html?_r=0.
[86] http://www.mediapost.com/publications/article/169317/ftcs-brill-do-not-track-means-do-not-collect-d.html#ixzz2Ym0RSXK8.
[87] CFO, Rob van Eijk, Article 29 Working Party.
[88] http://www.w3.org/wiki/Privacy/TPWG/Change_Proposal_Short_Term. Dan Auerbach of EFF has proposed a one-week retention period.
[89] Consensus Action Summary, http://op.bna.com/der.nsf/id/sbay-97jv8n/$File/aa130509-2.pdf.
[90] CFO, Lee Tien and Dan Auerbach, Electronic Frontier Foundation.
[91] Jonathan Mayer wrote: "I would encourage participants following this topic to read a blog post on privacy-improved advertising measurement that I co-authored with Arvind Narayanan." http://lists.w3.org/Archives/Public/public-tracking/2012Jul/0124.html.
[92] http://www.w3.org/2013/07/03-dnt-minutes.
[93] CFO, Shane Wiley, Yahoo! There is also mention of the term "unique" in the comments by Vinay Goel of Adobe. It appears that his comments speak to the importance of allowing short-term caching or other short-term collection, which, as discussed above, would be addressed in a separate provision of the June text or a possible change proposal.

[94] CFO, David Wainberg, AppNexus.
[95] CFO, John Simpson, Consumer Watchdog.
[96] CFO, Jonathan Mayer, Stanford University.
[97] Peter Swire, "The Need for Privacy Protections: Is Industry Self-Regulation Adequate?", U.S. Senate Commerce Committee, June 28, 2012, http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4c73aa3c-5626-42d6-b6fe-31e3ec6ad1ca.
[98] CFO, Dan Auerbach, Electronic Frontier Foundation.
[99] CFO, Brooks Dobbs, KBM Group; CFO, Mike O'Neil, Baycloud Systems Limited; http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0234.html.
[100] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0320.html.
[101] CFO, Jonathan Mayer, Stanford
[102] CFO, Aleecia MacDonald, Stanford.
[103] CFO, Mike O'Neill, Baycloud Systems Limited.
[104] CFO, Justin Brookman, Center for Democracy and Technology.
[105] http://lists.w3.org/Archives/Public/public-tracking/2013Jun/0261.html.
[106] CFO, Justin Brookman, CDT.
[107] See Peter Swire, *The Need for Privacy Protections: Is Industry Self-Regulation Adequate?*, U.S. Senate Commerce Committee (June 28, 2012), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4c73aa3c-5626-42d6-b6fe-31e3ec6ad1ca (reporting commitment from DAA General Counsel Stu Ingis to address these exceptions.). Swire was also on a panel at the International Association of Privacy Professionals conference in Washington, D.C., in March 2013 when Stu Ingis repeated this commitment.
[108] E.g., CFO, Shane Wiley, Yahoo!; CFO, Lou Mastria, Digital Advertising Association(DAA).; CFO, Chris Mejia, Interactive Advertising Bureau (IAB); CFO, Keith Scarborough, Association of National Advertisers (ANA); CFO, Alan Chapell, Chapell & Associates; CFO, Brad Kulick, Yahoo!; CFO, Brooks Dobbs, KBM Group; CFO, David Wainberg, AppNexus; CFO, Peter Kosmala, American Association of Advertising Agencies (4A's); CFO, Jack Hobaugh, Network Advertising Initiative (NAI).
[109] CFO, Mike O'Neill, Baycloud Systems Limited. Dan Auerbach of EFF similarly said: "We fear that a widely adopted standard will be so close to the status quo that users will see no value to DNT." CFO, Dan Auerbach, EFF.
[110] See Peter Swire, *The Need for Privacy Protections: Is Industry Self-Regulation Adequate?*, U.S. Senate Commerce Committee (June 28, 2012), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4c73aa3c-5626-42d6-b6fe-31e3ec6ad1ca (reporting commitment from DAA General Counsel Stu Ingis to address these exceptions.). Swire was also on a panel at the International Association of Privacy Professionals conference in Washington, D.C., in March 2013 when Stu Ingis repeated this commitment.
[111] CFO,Lou Mastria, DAA Brooks Dobbs, KBM Group; CFO, Rachel Thomas, DMA; Jack Hobaugh, NAI; CFO, Keith Scarborough, ANA; CFO, Brad Kulick, Yahoo!; CFO, David Wainberg, AppNexus.
[112] CFO, David Wainberg, AppNexus.

[113] http://www.networkadvertising.org/.
[114] Peter Swire, *How to prevent the 'Do Not Track' Arms Race*, Wired (April 24, 2013), http://www.wired.com/opinion/2013/04/do-not-track/.
[115] CFO, Shane Wiley, Yahoo!; CFO, Alan Chapell, Chapell & Associates. CFO, Jeff Wilson, AOL; CFO, Jack Hobaugh, NAI.
[116] http://www.w3.org/2013/07/03-dnt-minutes.
[117] CFO, Shane Wiley, Yahoo!.
[118] http://lists.w3.org/Archives/Public/public-tracking/2013Jul/0365.html.
[119] CFO, Alan Chapell, Chapell & Associates.
[120] CFO, Lou Mastria, DAA. CFO, Shane Wiley, Yahoo!; CFO, Jeff Wilson, AOL; CFO, Peter Kosmala, 4A's; CFO, Jack Hobaugh, NAI.
[121] http://www.w3.org/wiki/Privacy/TPWG/Change_Proposal_Deidentification
[122] http://lists.w3.org/Archives/Public/public-tracking/2013Jun/0270.html.