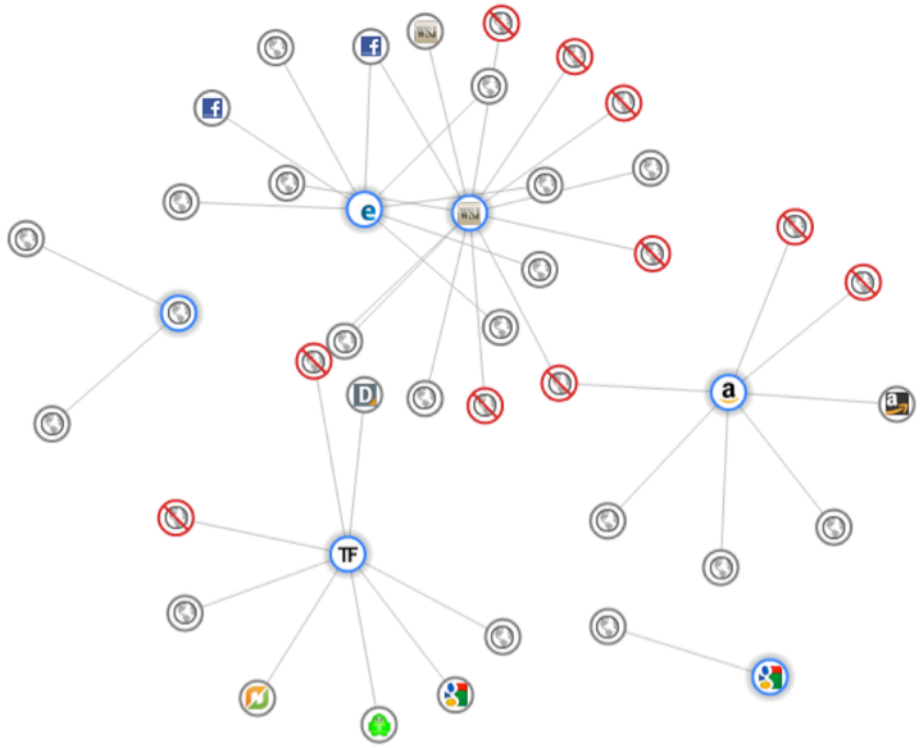
Who is following me? Tracking the trackers

A background paper for a workshop co-organised by the Council of Europe and the Internet Society at the Internet Governance Forum in Baku, Azerbaijan in November 2012.[1]



Introduction

Interest in online tracking as a policy issue spiked with the release of the Preliminary Federal Trade Commission Staff Report in December 2010[i] calling for a "do not track" mechanism, the launch of the W3C Tracking Protection WG[ii] and the recent entry into force of the so-called European "Cookie Directive" provisions[iii]. However, the actual and potential observation of individuals' interactions online has long been a concern for privacy advocates and others. Much of the policy attention is currently focused on cookies used to track users to build profiles for more targeted advertising, but some of the more difficult issues are:

- How to deal with less-observable tracking (e.g. browser and device fingerprinting, monitoring of publicly disclosed information)

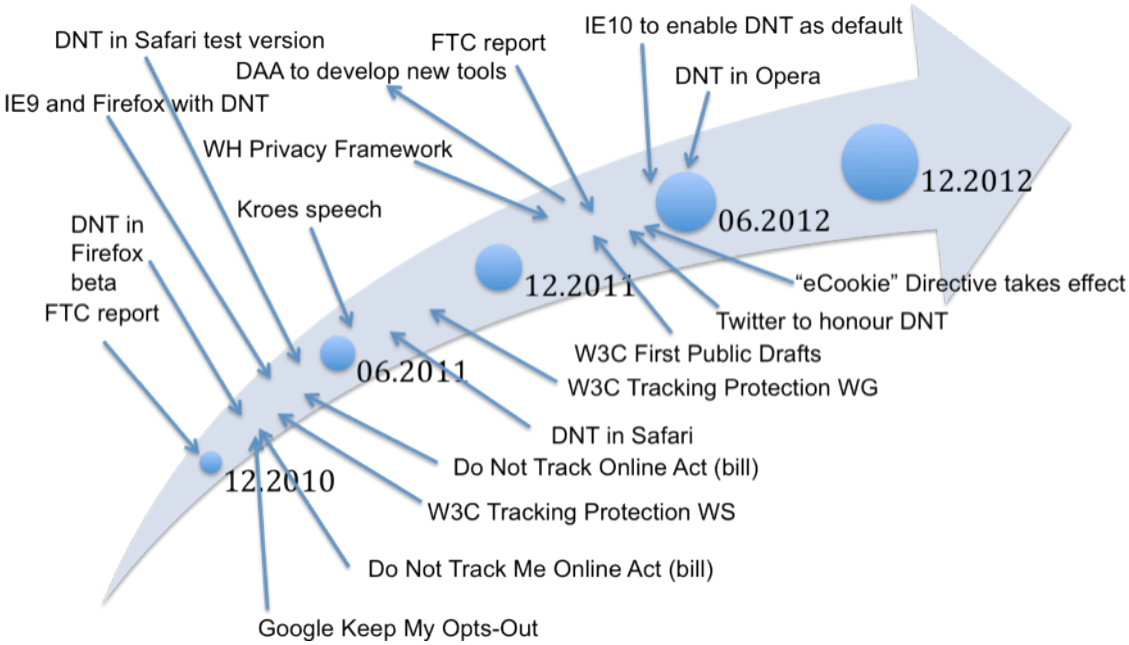
[1] The picture is a screenshot of a graph displaying trackers and their relationships produced by a Google Chrome extension known as "Collusion". This graph was produced after only visiting six sites. The crossed-out circles are trackers that the extension has blocked.

- DNT is only a mechanism for users to express a preference – How then do we provide a guarantee that the preference will be honoured?

- How to develop laws that accommodate different tracking scenarios using different technologies (some of which are yet to be imagined), for example:
    - Different entities (law enforcement, companies, etc.);
    - Different and sometimes multiple purposes (security, personalising user experience, targeted advertising, malicious activity; etc.);
    - First-party and third-party tracking
    - Single site and multiple site tracking

The companion piece is considering how personal data may or may not be retained, used or disclosed after it has been collected – i.e. what happens post-tracking?

Some developments regarding "Do Not Track" and Directive 2002/58/EC



In December 2010, the US Federal Trade Commission issued a report – *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers*[iv] - stating, among other things:

> *… Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as "Do Not Track." Such a universal mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation. The most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those choices.*
>
> *Such a mechanism would ensure that consumers would not have to exercise choices on a company-by-company or industry-by-industry basis, and that such choices would be persistent. It should also address some of the concerns with the existing browser mechanisms, by being more clear, easy-to-locate, and effective, and by conveying directly to websites the user's choice to opt out of tracking. …*

Shortly after the US FTC released its report, the major browser vendors started adding an optional "Do Not Track" feature to allow users to send a request (via HTTP referrer header) to web servers that they not be tracked (i.e. a means of expressing a preference not to be tracked):

- February 2011: Mozilla added the feature to Firefox 4 beta[v]
- March 2011: Microsoft released Internet Explorer 9 (IE9) with the feature[vi]
- March 2011: Mozilla releases Firefox 4[vii]
- April 2011: Apple added the feature to a test version of Safari[viii]
- July 2011: Apple releases Mac OX Lion[ix]
- June 2012: Opera included the feature in its release of Opera 12[x]
- Later in 2012: Google is expected to implement this feature in Chrome[xi]

In February 2011, Google released a Chrome extension called "Keep My Opts-Out" designed to allow users to permanently opt-out of tracking and behavioural advertising by those companies participating in the program.[xii]

On 18 February 2011, Representative Jackie Speier introduced a new bill to the US Congress – the *Do Not Track Me Online Act of 2011*.[xiii]

In April 2011, the W3C hosted a Workshop on Web Tracking and User Privacy.[xiv] An outcome of this workshop was the creation of the W3C Tracking Protection Working Group[xv], which seeks to standardize the technology and meaning of Do Not Track and Tracking Selection Lists. This work is part of the W3C Recommendation Track. A W3C Recommendation is "a specification or set of guidelines that, after extensive consensus-building, has received the endorsement of W3C Members and the Director. W3C recommends the wide deployment of its Recommendations".[xvi]

On 9 May 2011, Senator John "Jay" Rockefeller introduced a new bill to the US Congress – the *Do-Not-Track Online Act of 2011*.[xvii]

On 22 June 2011, Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Online gave a speech calling for a broader discussion regarding "Do Not Track"[xviii]:

> *More specifically, I think we should collectively pay more attention to the emerging 'do-not-track' technologies – or DNT for short.*
>
> *DNT is simple: users can instruct their device or application to accompany all network requests with an indication that they do not want to be tracked. Service providers need to react to such explicit requests.*
>
> *DNT has a lot of potential because it can apply:*
>
> *First, to all networked devices and applications*
>
> *Second, to all types of tracking and*
>
> *Third, to all purposes of tracking.*
>
> *DNT is already deployed in some web browsers. And some web businesses say they honour it.*
>
> *But this is not enough. Citizens need to be sure what exactly companies commit to if they say they honour DNT. For example, there is an important difference between a commitment not to record tracks and a commitment not to use them for a specific purpose once recorded. When this is solved more users will deploy DNT – and it will become simpler – and companies will go along. So we are looking at a virtuous circle.*
>
> *How do we get there? We need a standard! We need to standardise how the DNT signal and the expected reaction should look. The standard must be rich enough for users to know exactly what compliant companies do with their information and for me to be able to say to industry: if you implement this, then I can assume you comply with your legal obligations under the ePrivacy Directive.*

I am sure regulators in other jurisdictions will want to do the same!

The internet is a global achievement and privacy is a global concern. So our technical approach to it must also be global, and fit the generative network.

Fortunately we do not start from scratch. Drafts for a DNT standard already exist. Therefore I am confident that a standardisation initiative for DNT can progress quickly. I am committed to supporting such an initiative and I invite my colleagues in the EU and elsewhere to join me. The US in particular is a most important partner in this and I am grateful that the Federal Trade Commission, which has already shown an interest in DNT, is represented here today at Commissioner's level. Indeed, I had a chance to discuss this with Commissioner Brill just before my speech. This event therefore is a good occasion to get going in earnest.

I urge all interested parties to come to the standardisation table. And I challenge you to agree a DNT standard by June 2012.

And, while I am on the subject, one group I would especially like to see taking part in this is the online advertising industry – because of its experience and because the self-regulation, which is currently based on cookie technology, will need to address DNT as well.

The W3C Tracking Protection WG started work in September 2011. The WG is developing a Tracking Preference Expression specification and Tracking Preference Expression Definition and Compliance specification. As at 10 July 2012, W3C Recommendations are projected to be ready by October 2012.[xix]

In February 2012, the White House published *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*[xx]. With respect to "Do Not Track", the document says:

> *… All of these mechanisms show promise. However, they require further development to ensure they are easy to use, strike a balance with innovative uses of personal data, take public safety interests into account, and present consumers with a clear picture of the potential costs and benefits of limiting personal data collection. …*

On 23 February 2012, the Digital Advertising Alliance (DAA) announced that "… it will immediately begin work to recognize browser-based choices with a set of tools by which consumers can express their preferences under the DAA Principles".[xxi]

On 13 March 2012, the W3C released a public Working Draft Tracking Preference Expression (DNT) specification[xxii] and a public Working Draft Tracking Compliance and Scope specification[xxiii].

In March 2012, Yahoo announced "… the implementation of a Do Not Track (DNT) header solution that will be accessible across Yahoo!'s global network by early summer … This site-wide DNT mechanism … will provide a simple step for consumers *to express their ad targeting preferences* to Yahoo!".[xxiv] (emphasis added)

On 26 March 2012, the US Federal Trade Commission released a new – *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers*, which states, among other things:

> *Like the preliminary staff report, this report advocates the continued implementation of a universal, one stop choice mechanism for online behavioral tracking, often referred to as Do Not Track. Such a mechanism should give consumers the ability to control the tracking of their online activities.*
>
> *…*
>
> *The Commission commends recent industry efforts to improve consumer control over behavioral tracking and looks forward to final implementation. As industry explores technical options and implements self-regulatory programs, and Congress examines Do Not Track, the Commission continues to believe that in order to be effective, 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 (e.g., preventing click-fraud or collecting de-identified data for analytics purposes).

The Council of Europe Steering Committee on Media and Information Society produced a Draft Committee of Ministers declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies (CDMSI(2012)002) in March 2012 stating, among other things:

Against this background, the Committee of Ministers:

b. fully supports member states' efforts to address the question of tracking and surveillance technologies and their impact on people's exercise and full enjoyment of fundamental rights and freedoms as well as their impact on society as a whole.[xxv]

In May 2012, Twitter announced that it would honour "Do Not Track".[xxvi]

On 31 May 2012, Microsoft announced that a "Do Not Track" feature in Internet Explorer (IE10) would be enabled by default.[xxvii] This announcement has been met with mixed reactions. For example, the Interactive Advertising Board (IAB) issued a response stating, among other things:

… We do not believe that default settings that automatically make choices ***for*** *consumers increase transparency or consumer choice, nor do they factor in the need for digital businesses to innovate and thrive economically. Actions such as these will undermine the success of our industry's self-regulatory program. Such actions also will constrain the flow of ad-supported digital content that informs, educates, entertains and delights consumers across the U.S. and the world.*[xxviii]

The Director-General of the Information Society and Media Directorate-General of the European Commission said, on 21 June 2012[xxix]:

Third, it is not the Commission's understanding that user agents' factory or default setting necessarily determine or distort owner choice. The specification need not therefore seek to determine the factory setting and should not do so, because to intervene on this point could distort the market.

Tools to reveal tracking and block Web tracking elements (some examples)

There are a large number of different browser plug-ins, add-ons and extensions to show users which sites are tracking their browsing activities, block and/or remove different types of tracking elements (e.g. HTTP cookies). Many of these are available at no cost to the user. Some examples include:

- Ghostery[xxx]
- Collusion[xxxi]
- Do Not Track Plus[xxxii]
- Better Privacy[xxxiii]

Tools to improve confidentiality of browsing (two examples)

HTTPS Everywhere, an extension for Firefox and Chrome, was produced as a result of a collaboration between The Tor Project and the Electronic Frontier Foundation.[xxxiv] For websites that support HTTPS, the extension helps users access the encrypted versions of those sites.

DuckDuckGo, described as a hybrid-browser, says it does not collect or share personal information. Further, it says it prevents search leakage (disclosure of search terms to other sites) and supports HTTPS searches.[xxxv]

Tor is "a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. … Individuals use Tor to keep websites from tracking them and their family members …. Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses …".[xxxvi]

Tools to demonstrate browser fingerprinting to users (an example)

Panopticlick, a research project of the Electronic Frontier Foundation, tests the uniqueness of the user's browser.[xxxvii]

Tools to illustrate what a user's browsing history may reveal to trackers (an example)

PrivacyBucket is a Chrome extension designed to illustrate how much trackers may be able to learn from a user's browsing history.[xxxviii]

PrivacyBucket is a Chrome extension for showing how much trackers can learn about you. Based on your browsing history, PrivacyBucket will compute an approximation for what different online trackers may learn about you, in terms of your demographic profile.

Grading systems (an example)

The trackingcookie.info extension was created during the Wall Street Journal Code-a-Thon on 13 April 2012. It provides a form of "Tracking Report Card", grading websites from A to F. The highest grade is awarded to first-party sites that:

- "do not allow a large amount of 3rd party networks to be called on their site (and do not let a lot of 3rd party networks to download tracking cookies on the visitor's browser)"
- "honor both "opt-out" cookies and "do not track" requests).[xxxix]

Tracking by Apps (an example)

Earlier this year, the *Wall Street Journal* analysed 100 Facebook apps to ascertain what data they sought from users[xl] and produced the results in an interactive graphic[xli]. The WSJ observed:

> *… Facebook requires apps to ask permission before accessing a user's personal details. However, a user's friends aren't notified if information about them is used by a friend's app. …*

Tracking users offline using public online data (an example)

Earlier this year, in an experiment designed to highlight privacy risks associated with public tweets, a Japanese columnist, following three Twitter profiles quickly found two of the three individuals to whom the profiles had been allocated in streets of the densely populated Japanese city of Shibuya.[xlii]

Uses for data obtained via online tracking

Ask the typical consumer what data obtained via online tracking is used for and they will probably respond with "advertising", behavioural advertising" or "targeted advertising". Yet, such data could be used for any number of purposes by any number of actors. Two other commonly cited use cases are: to improve users' Web experience (e.g. an airline site remembering the user's country location and preferred language) and to enhance security (i.e. an additional means to assess

whether the user is who he or she purports to be, e.g. a Web-based email provider remembering from which approximate geographic location the user typically accesses his or her email).

In the news in late June 2012, there were reports that Orbitz Worldwide Inc., an online travel agency, had started displaying more expensive options to Mac users than to PC users because its research had found that Mac users typically spend more per night on hotel rooms. Orbitz also makes assumptions based on how users arrive at their site. For example, if they enter through an aggregator like kayak.com, they are thought to be more price-sensitive than users who arrive from review focused sites such as tripadvisor.com.[xliii]

In the workshop, we will explore further how tracking data is or may used.

Actors in the online tracking ecosystem

The number and range of actors involved in the online tracking ecosystem continues to grow and evolve at a rapid pace. This is a non-exhaustive list (in no particular order):

- Internet users
- Internet service providers
- Data collectors (first and third+ parties)
- Data brokers
- Data aggregators and analysers
- Data users
- Online advertisers
- Browser vendors
- Search engine providers
- Device manufacturers
- Operating system providers
- Data auctioneers
- Government
- Developers of tracking technologies and techniques
- Developers of tools to reveal and/or prevent tracking
- Internet technical community
- Privacy advocates
- Compliance vendors

In the workshop, we will consider the various actors involved and their respective roles.

Some additional resources

Council of Europe Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling[xliv] and Convention 108[xlv]

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[xlvi]

Guidance regarding the application of Article 5(3) of Directive 2002/58/EC

- CNIL revised guidance – Ce que le "Paquet Télécom" change pour les cookies (23 April 2012)[xlvii] (highlights in English, courtesy of Bird & Bird[xlviii])

- UK ICO revised Guidance on the rules on use of cookies and similar technologies (May 2012)[xlix]

- Article 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption (adopted on 7 June 2012)[l]

Information regarding the work being undertaken by the W3C Tracking Protection WG

- W3C Tracking Protection WG landing page[li]
- 8 September 2011: "Do Not Track" standards for the Web: The work is starting.[lii]
- 2 February 2012: Progress and support for Do Not Track in Brussels[liii]
- 26 April 2012: W3C Blog: The state of Do Not Track[liv]
- 20 June 2012: W3C Blog – Tracking Controversy[lv]
- 26 June 2012: W3C Blog – Report from Bellevue: meaningful advances on Do Not Track[lvi]

Papers submitted for the W3C Workshop on Web Tracking and User Privacy in April 2011[lvii]

DoNotTrack.US website[lviii]

- Annotated Bibliography of Related Work[lix]

Note: Please feel free to send us pointers to other relevant work, initiatives, articles and opinions concerning online tracking at info-online-tracking@isoc.org.

Date: 11 July 2012

Endnotes:

[i] *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
[ii] http://www.w3.org/2011/tracking-protection/
[iii] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications) (see Article 5(3) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML)
[iv] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
[v] http://www.eweek.com/c/a/Security/Mozilla-Adds-Do-Not-Track-Feature-to-Firefox-4-Beta-553815/
[vi] http://securitywatch.pcmag.com/web-browsers/298596-microsoft-turns-on-do-not-track-by-default-in-ie10
[vii] http://www.techspot.com/news/42908-mozilla-releases-firefox-4.html
[viii] http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html
[ix] http://www.independent.co.uk/life-style/gadgets-and-tech/apples-lion-roars-onto-computers-with-1-million-downloads-in-a-day-2318755.html
[x] http://www.pcmag.com/article2/0,2817,2405787,00.asp
[xi] http://www.reuters.com/article/2012/05/18/us-twitter-privacy-idUSBRE84H0KF20120518
[xii] http://www.eweek.com/c/a/Security/Google-Chrome-Keep-My-Opt-Outs-Joins-Fight-Against-Online-Tracking-577479/
[xiii] http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.00654: (Bill - http://thomas.loc.gov/cgi-bin/query/z?c112:h654:)
[xiv] http://www.w3.org/2011/track-privacy/report.html
[xv] http://www.w3.org/2011/tracking-protection/
[xvi] http://www.w3.org/2005/10/Process-20051014/tr#q74
[xvii] http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.00913: (Bill - http://thomas.loc.gov/cgi-bin/query/z?c112:S.913:)
[xviii] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/461
[xix] http://www.w3.org/2011/tracking-protection/
[xx] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[xxi] http://www.aboutads.info/resource/download/DAA_Commitment.pdf (For the DAA Self-Regulatory Principles for Online Behavioral Advertising, see http://www.aboutads.info/obaprinciples and for the Self-Regulatory Principles for Multi-Site Data, see http://www.aboutads.info/msdprinciples)
[xxii] http://www.w3.org/TR/tracking-dnt/
[xxiii] http://www.w3.org/TR/tracking-compliance/
[xxiv] http://pressroom.yahoo.net/pr/ycorp/231249.aspx
[xxv] https://encrypted.google.com/url?sa=t&rct=j&q=council+of+europe+%2B+tracking&source=web&cd=3&ved=0CFAQFjAC&url=http%3A%2F%2Fwww.coe.int%2Ft%2Fdghl%2Fstandardsetting%2Fmedia%2FCDMSI%2FCDMSI(2012)002_en.pdf&ei=wyT9T43QLfTP4QT5vPCVBw&usg=AFQjCNGd9aNHF_1EKQXNK401VVyynKVY4w&cad=rja
[xxvi] http://www.reuters.com/article/2012/05/18/us-twitter-privacy-idUSBRE84H0KF20120518
[xxvii] http://securitywatch.pcmag.com/web-browsers/298596-microsoft-turns-on-do-not-track-by-default-in-ie10

[xxviii] http://www.iab.net/InternetExplorer
[xxix] http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0604/Letter_to_W3C_Tracking_Protection_Working_Group.210612.pdf
[xxx] http://www.ghostery.com/
[xxxi] https://addons.mozilla.org/en-US/firefox/addon/collusion/
[xxxii] http://www.abine.com/dntdetail.php/
[xxxiii] https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/
[xxxiv] https://www.eff.org/https-everywhere/
[xxxv] https://duckduckgo.com/privacy.html
[xxxvi] https://www.torproject.org/about/overview.html.en
[xxxvii] https://www.eff.org/https-everywhere/
[xxxviii] https://github.com/mfredrik/Privacy-Bucket/wiki
[xxxix] http://www.trackingcookie.info/
[xl] http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html
[xli] http://online.wsj.com/article/SB10001424052702303302504577328363924309098.html
[xlii] http://www.mediabistro.com/alltwitter/japanese-twitter-stalker-experiment_b19850#more-19850
[xliii] http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html
[xliv] https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383
[xlv] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[xlvi] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
[xlvii] http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/
[xlviii] http://www.twobirds.com/English/News/Articles/Pages/CNIL_reissues_guidance_analytic_cookies.Aspx
[xlix] http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx
[l] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
[li] http://www.w3.org/2011/tracking-protection/
[lii] http://www.w3.org/QA/2011/09/do_not_track_standards_for_the.html
[liii] http://www.w3.org/QA/2012/02/support_for_do_not_track_brussels.html
[liv] http://www.w3.org/QA/2012/04/the_state_of_do_not_track.html
[lv] http://www.w3.org/QA/2012/06/tracking_controversy.html
[lvi] http://www.w3.org/QA/2012/06/report_from_bellevue_meaningfu.html
[lvii] http://www.w3.org/2011/track-privacy/papers.html
[lviii] http://donottrack.us/
[lix] http://donottrack.us/bib/