# Do-Not-Track, Doctor Who, and a Constellation of Confusion

**Lauren Weinstein**
lauren@vortex.com
http://lauren.vortex.com

**April 30, 2011**

**Executive Summary:** Contrary to arguments made by many proponents of Internet "Do-Not-Track" concepts, there are vast complexities involved in any rational approach to this area. Can *Doctor Who* help us understand?

---

In the long-running BBC television series *Doctor Who*, a running gag for decades has been the confusion of characters discovering that the Doctor's spacetime travel vehicle, the TARDIS, appears externally to be a tiny British police call box (not much larger than a traditional AT&T phone booth), but due to its "transdimensional" nature, is revealed to be vastly larger on the inside.

During an episode of the show's 70s-era incarnation, actor Tom Baker -- considered by many to have portrayed the quintessential version of the *Doctor Who* lead role, uses a pair of small boxes to explain how misleading it can be to judge internal complexities simply from their seemingly obvious outside similarities and appearances.

A striking parallel with this scene can be drawn when we consider the ongoing arguments regarding Internet do-not-track concepts, technologies, and proposed legal requirements. As in *Doctor Who*, assumptions made based on first impressions can turn out to be

overly simplistic and spurious in the extreme.

An obvious issue in this regard are oft-quoted, but extremely faulty attempts to equate “do-not-call” phone solicitation prohibitions with Internet do-not-track proposals.

The fallacy of trying to liken these two widely divergent concepts should be apparent immediately.

Do-not-call is a “binary” creation, like an on-off light switch. Either someone calls your phone to try sell you something -- or they don’t.  Simple enough.

But what does “tracking” even mean in the context of demands for Internet do-not-track systems?

Most of the attention seems to be focused on usually aggregated and often anonymized data correlation used for Web page ad display personalization services, which typically seek to be less intrusive to Web viewers than would be random ads of much less likely interest to any given person.

Some ad server networks already provide the means for Web viewers to select and control preferences for these ads -- options that typically are not present with traditional media advertising.

To be sure, there are elements in the do-not-track movement who are using do-not-track as a sort of “code” for simply not wanting to view Web-based advertising at all.  Calls for do-not-track are not infrequently accompanied by the promotion of browser ad blocking plugins or extensions, and an implicit (or even explicit) refutation of the compelling argument that ads are important to maintain the availability of the largely “free” Web services model that we’ve all come to enjoy.

Of especial concern is the implication that ad personalization is somehow inherently evil or dangerous. This characterization seems particularly erroneous when we compare with other Internet tracking-related issues that by and large have not been the focus of most current do-not-track promoters.

Even while some divisions of government are proselytizing for the rapid adoption of risky and overly simplistic do-not-track mechanisms that are more akin to sledgehammers than balanced control methodologies, and aimed particularly at ad personalization networks -- others in government are pushing hard for vast and comprehensive data retention laws that would require ISPs and Web services to record and maintain detailed records of virtually all Web browsing, email, and other activities.

Unlike the care employed in typical major ad personalization networks to prevent the association of related data in a manner that could be used beyond the stated purpose of ad presentations, government-mandated data retention regimes nearly inevitably require that all activity data be directly tied to individual users in a manner subject to full identification and reporting "on demand" of authorities, sometimes even without the requirement of warrants or other court orders.

Why is there such a focus on do-not-track in the relatively innocuous ad serving sector, but often so much hypocritical disregard of government's desire for encompassing tracking in other contexts that carry enormously larger potentials for abuses?

One likely reason is purely commercial. A major player in the Web ad marketplace is obviously Google, and some of Google's competitors, either directly or via veiled "astroturf" confederates, appear to have seized on the concept of simplistic do-not-track

populism as a convenient strategy to try undermine various Google initiatives that have negatively affected those competitors' bottom lines.

A more insidious possibility also exists, however. The do-not-track focus by government targeting commercial Web ad serving systems may tend to distract attention -- intentionally or not -- from government's own largely behind-the-scenes push not only for broad Web user data retention as discussed above, but also for access to users' encrypted voice and other Internet-based communications.

Encouraging the deployment of pitchforks and torches against Google may serve quite nicely in a public relations and press management sense, to divert popular thought away from those in government who are actively attempting to establish deep and permanent access to Web users' activities and data, again often on a warrantless basis.

There are also individuals and groups who fully understand the inherent complexities involved in any reasonable discussion of do-not-track, but have chosen, for various reasons, to promote simplistic do-not-track systems on what I view to be a seriously flawed and inappropriate "doing anything is better than doing nothing" basis, despite the significant and pervasive risks inherent in such an approach.

As we can see, the factors that are integral to any sensible discussion of do-not-track are numerous and complex.

Attempts to simplify related arguments, as in the manner of comparisons to do-not-call lists, only further muddy an already complicated situation.

In small towns of the past, the proprietor of a general store might know his customers so well that he could guess most of their needs as soon as they walked in the door, and would be expected to offer other products that he or she surmised the customer might reasonably be interested in obtaining. Such "personalization" wouldn't be condemned, but rather would typically be much appreciated by the vast majority of patrons. On the other hand, if that same store owner was caught peeping in their customers' windows at night, the reactions would be very negative. Different situations quite understandably yield different responses.

Rather than view do-not-track and tracking in general as binary choices, or even as an overly simplistic one-dimensional continuum -- with "no tracking" and "tracking" at the good and evil ends of the spectrum respectively -- a multidimensional and so significantly more nuanced view would seem to make a great deal better logical sense.

For each of us, our comfort levels with "tracking" as it may be most broadly defined -- both in Internet and non-Internet contexts -- will vary widely depending on specific details and circumstances.

Imagine an n-dimensional graph, with different categories of tracking, services, and situations arrayed along the various axes. Throughout this complex space we can envision a constellation of points where various interests and concerns intersect in different situations involving our personal lives, business lives, commercial transactions (both "brick and mortar" and Internet), Digital Rights Management (DRM) considerations, banks, stores, credit cards, political parties, voting data, and so on.

The shape of that multidimensional constellation -- presumably much easier for the lead character of *Doctor Who to* visualize than for you or me -- will at any given moment in time represent the

intricate nature of our willingness to interact with the associated entities and services in an array of ways, including the universe of personalization services in particular, and broader definitions of tracking in general.

The upshot of all this seems quite clear. Do-not-track in actuality encompasses an immensely heterogeneous mosaic of issues and considerations, not appropriately subject to simplistic approaches or "quick fix" solutions.

Approaching this area without a realistic appreciation of such facts is fraught with risks and the potential for major undesirable collateral damages to businesses, organizations, and individuals.

Attempts to portray these controversies as "black or white" topics subject to rapid or in some cases even unilaterally imposed resolutions may be politically expedient, but are ultimately both childish and dangerous. This is especially true when various concerned stakeholders become positioned in mutually antagonistic positions in key respects, due to a lack of effective channels for associated communications and discussions, or an unwillingness by some involved parties to forgo unyielding demands or ulterior motivations.

Above all, we should endeavor to remember that tracking issues both on and off the Internet are in reality part of a complicated whole, a multifaceted set of problems -- and very importantly -- potentials as well.

The decisions that we make now regarding these issues will likely have far-ranging implications and effects on the Internet for many years to come, perhaps for decades.

Unfortunately, we can't just hop into the *Doctor Who* TARDIS,

zoom forward a bit in time, and observe how well (or how horribly) rushed attempts at addressing this area have turned out.

So we must depend on ourselves instead.  In particular, if we seriously wish to have the best possible Internet for everyone, we should steel ourselves to eschew politics, emotions, and "ad hoc" proposals or implementations, and instead come together to discuss these issues as adults in an ordered and reasoned manner . If we truly have at heart the best interests of the Internet community, and the global community more generally, not only will they both ultimately appreciate our due diligence, but future generations will likely thank us as well.