

# CNet News.com Writers Demonstrate Desire For Sensationalism And Poor Technical Understanding

Posted At : January 5, 2006 2:35 PM | Posted By : Ben Forta

Related Categories: ColdFusion

CNet's News.com is running a story by staff writers Declan McCullagh and Anne Broache with the sensational title **Government Web sites are keeping an eye on you.**

The key points of the article are:

- A 2003 directive makes it illegal for federal agency web sites to track user activity or monitor user behavior.
- Some government agencies are using cookies on their sites (although there is no report of what those cookies are and what it is that is stored in them).
- "Many of the cookies appearing on the errant Web sites were generated by ColdFusion, the popular Web authoring tool ... which sets them to expire about 30 years in the future".
- WebTrends and ColdFusion are the only products mentioned as the ones creating cookies.
- The article does not actually state that ColdFusion is doing bad things (with the exception of "one Smithsonian Institution Web staffer, who initially denied the existence of persistent cookies detected by CNET News.com on the National Air and Space Museum's site, said that ColdFusion settings were probably to blame"), but there is a sense of guilt-by-association here.

This is yet another alarmist article, decrying the presence of cookies without any explanation of what they are used for and what is stored in them. Blanket statements about cookies are irresponsible. But that is not my real concern here. The bigger issue is ColdFusion, cookies, and "30 year" persistence.

So, what are these "30 year" cookies? Where does that number come from, and what does it actually mean?

First let me make this very clear: ColdFusion does not store any data in cookies. Ever.

But ColdFusion does create cookies for you. How? If you use `CLIENT` or `SESSION` variables then identifier cookies are created. These contain an id and a token (the combination of which make up a unique client identifier) but no actual data is ever stored in cookies. These cookies are persistent cookies, they don't expire, although the `SESSION` or `CLIENT` that they identify does indeed expire.

Granted, the presence of `CFID` and `CFTOKEN` (or `jsessionid`) cookies may alarm some users, but the fact of the matter is that these cookies present neither a privacy nor a security concern.

This is all explained quite clearly in the ColdFusion documentation. As is how to a) maintain session-state without using cookies at all, and b) how to make these identifier cookies persist only until the end of the browser session.

So, to clarify, ColdFusion does create cookies if you use session-state management, but these store simple identifiers (a number or a UUID, and no actual data), and cookie use can be disabled altogether (although this is not the default behavior).

So, is there an actual risk here? Can cookies contain more sensitive information and persist for "30 year"?

Well, no, not if they are ColdFusion generated cookies. But developers can indeed opt to do so.

The ColdFusion <cfcookie> tag is used to create (and update and delete) cookies. ColdFusion developers can use this tag to store data in cookies, and they can (although they should not) store sensitive data in these cookies. The <cfcookie> tag EXPIRES attribute specifies how long the cookie should persist for. By default, cookies expire when the browser closes. But it is also possible to specify an actual date and time for them to expire, as well as "never" which (as the documentation explains) makes the cookie expire "in 30 years from the time it was created (effectively never in web years).".

In other words, ColdFusion developers can create cookies that do indeed have a "30 year" lifetime, but that is not the default behavior, that is something a developer must consciously decide to make happen. As such, this scenario cannot be what the story refers to (ColdFusion tracking occurring without anyone knowing that it was going on).

So, we are back to CFID and CFTOKEN, the identifier cookies, which we know store no user data and do no monitoring.

Now, it could be argued that ColdFusion should not use cookie identifiers by default. There are two primary ways to identify sessions, cookies and URL tokens, and the default could indeed be to use the latter. This would be a valid suggestion, but as any developer who has opted to go down this road knows, this makes development far more complex. As such, I believe that the default behavior is what it should be (because, the identifier cookies do not store anything sensitive, they store no data at all).

It could also be argued that the default lifetime of these cookies should be lower. That is something we need to consider, although I suspect that as dramatic as "30 year" sounds, the same article would have been written even for a shorter duration.

The only way around this (without defaulting to URL tokens) would be for the identifier cookies to be browser cookies (expiring when the browser closes), and that is an option worth considering. This would not actually make any real difference (because, once again, these are identifier cookies only), but it could help placate ignorant alarmists.

But ColdFusion is still creating cookies. Do these violate the **OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002**?

The text reads: "*agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet*". It does not prohibit all persistent cookies, only those used to "*track visitors' activity on the Internet*". The text does not explain what "track" actually means, but the context is clear, cookies are prohibited when used for the tracking of user activity. Indeed, the text goes on to say that persistent cookies may be used (subject to approval and authorization) so long as the agency posts "*clear notice in the agency's privacy policy of the nature of the information collected, the purpose and use for the information, whether and to whom the information will be disclosed; and the privacy safeguards applied to the information collected*". This clarifies things quite a bit, and explains what the concern is; the collection of information (and possible subsequent disclosure).

ColdFusion's identifier cookies track nothing, they identify a session which quickly times out (the default time out is 20 minutes, and the default server imposed maximum is 2 days). No data is collected, there is no risk of future disclosure, there is no tracking. And as such, these identifier cookies do not violate the privacy provisions!

With all of this in context, consider the following quotes from the story:

- *"Many of the cookies appearing on the errant Web sites were generated by ColdFusion, the popular Web authoring tool. When the software creates certain types of cookies, it automatically assigns them a default persistent setting." The only cookies that persist by default are the identifier cookies, which store no data and do no tracking.*
- *"Many agencies appeared to have no inkling that their Web sites were configured to record the activities of users." Configured to record the activities of users?*
- *"Representatives at several agencies said they were astonished to see cookies on their Web sites, and they blamed their Web designer's lack of understanding of ColdFusion's default settings." Again, if developers did not put the cookies there, then the only cookies are the identifier cookies.*

My big problem with this story is that it leaves the impression that ColdFusion performs tracking and stores data, and that this occurs whether or not developers are aware of it. And this is just blatantly false!

Unless a developer opts to do so, there is no recording of user activity, there is no sensitive data stored in cookies, and there is no risk or violation of federal directives. It is as simple as that.

By weaving together partial facts, incomplete explanations, and tales of panicked reactions, Declan McCullagh and Anne Broache have traded journalist integrity and technical understanding for ignorant alarmist sensationalism. They should be ashamed of themselves!