All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Tracking you

We recently started to experiment with tracking you as you use our sites and as we send you marketing material. As a big fan of transparency, I thought I would let you know all about it.

We don't use cookies

I always thought the whole cookie thing was ridiculous. I didn't like placing (or allowing to be placed) content on user machines, and I thought the cookie thing was ridiculous in any case. So we never used cookies, although some of the sites hosting our servers might have at some point, without our permission. I don't actually know of any that did, but just saying…

We run our own servers – sort of

I used to physically purchase computers and pay for fixed IP addresses in my home to support remote access to content. This starting in the late 1990s, and going up till a few years back when we went to servers at 3rd party providers. I always preferred to not have to depend on someone else for whatever, but I eventually gave it up because it costs less and works better to let the 24x7 server farms do the job instead of me waking up in the middle of the night to service a computer failure or Internet outage.

We use a GoGDaddy service for one of our Web servers (all.net and several other domain sites are there), and we use AWS for hosting our servers that remain under my code control. When I say code control, I mean that for the most part I control the software above the OS level, including what's installed, internal firewalls, applications, etc.

So we don't have to share with others

And we don't. We decide long ago that we wouldn't (and so far haven't) sold or otherwise exchanged user information with 3rd parties. To the extent we gather it we do so for our own purposes, mostly just making sure things keep working and seeing what's out there coming at us. As a result, we don;t have all the advantages that others have of gaining from the big data they get about you. But we do want to see how well what we do works. So we have things like logs and audit trails.

So I decided to try something

I wanted to see how well the various emails and Web postings, etc. were doing in terms of generating actual readers for our free (to read) content. So I decided to add a tracker capability to find out how things are going and to do metrics on our outreach.

I did this by a simple method that stores nothing on your computer. All it does is use URLs that includes information like where we posted a message (e.g., LinkedIn) and when, along with a few identifiers for associating it with specific things we do. When you click (or automatically download an image or some such thing), we can attribute it to the cause. If you try to change something, we will know the tracking is no good, and it might mean you don't get whatever you clicked on, but rather a "don't do that sort of thing here" message or some such thing.

What did it show me?

Of course I don't completely know yet. But so far it has shown me several things I have started to see…

- The mechanisms between here and there keep changing stuff
  - I eventually have moved (and continue moving) toward encoding everything I can in the URI fields into hex digits because other than 0-9 and A-Z, lots of mechanisms try to alter the content of fields in Web requests. I think this is overly aggressive filtering and rewriting for the different criteria of different mechanisms along the way. But it is clearly a case of altering what is sent, which to me is breaking the trust we could otherwise have in the mechanisms being true to what is sent in terms of what is received. In short, if ot came from the Internet, it likely has been changed en route. And don't imagine SSL changes anything about this.
- It's a pain to try to track everything, so pick what you want to know
  - I did a few experiments with setting up a separate tracking mechanism for each of lots of items in a single email or posting. It's really about instrumentation. You have to see what you can see to see what you want to see, and then you can ignore the rest, or in the case of trackers, just never shine a light on it. Selective blindness is useful here, and frankly, I don't really want all that data on you. Yes, I know I could use it to my advantage to try to get something from you, but really, all I want is to learn about things and share my learning with others in the hopes it will make a better world for all of us. And I do not case what you had for breakfast or what type of pajamas you wear.
- Some people are just nasty and impolite
  - This is not a new lesson. Ever since I have been looking at logs, I have seen stupid so-and-sos who decide to swear at me in the log files by adding something abusive to their Web requests, or … lots of other things. I don't want to give you ideas of how to be more of a pain to others by listing all of them. The worst of them is the folks who come to my Web sites, read my free and open content, and when I try to email them to see if there is anything they are interested in or that I can help them with, tell me I am doing something bad to them by truthfully telling them that I saw their usage, and decide to report me to the self-appointed spam-XXX-whatevers who then try to block me from communicating with you. A little bit of niceness should always be present, and it would be even better if folks would look at the world from the other person's perspective from time to time.
- There is a big difference between the platform claims and the desired realities
  - It should not be a surprise that when LinkedIn tells you you have thousands of views of your postings (sent to they claim millions of people on their lists), only perhaps less than 1% ever actually look at what they supposedly saw. I only pick on them because that's where I did the test. I'm sure others do the same sort of thing, and I have done investigations that showed this to be so.

Conclusions

As you read this, I might be tracking you. But I am not here to hurt you. So take it easy.

