

PLEASE DONT PASS THE COOKIES OR JUST "COOKIES"

by Sasha Cavender, Freelance Journalist

"Cookies" technology is just one example of quietly invasive technology that's being used. It's only the tip of the iceberg. The vast majority of web users have NO idea it exists, or that it's being used like a 'reverse encryption' to secretly tag them, fingerprint them as they travel around the Web. They think they're following their curiosity. They don't know that ISP's and web site owners are following *them*.

When consumers are told, they are often shocked. Outraged. First there's disbelief, then they feel violated. It's like schoolgirls who are suddenly told someone's been staring down at their black patent leather shoes, not out of shyness, but to see their underwear. Consider stepping out of the shower, and seeing an intruder right there, watching you. If you and I are talking, standing next to one another and I step forward, you will automatically step back - because I have invaded your personal space. It's psychological, not just physical.

People in the industry often say, "Oh, it's not that bad." People outside the industry - ordinary Internet users say "It's *that bad*". Because, they believe the net is a huge public open space and marketplace, where they can wander unnoticed and anonymous as if they were on a busy street in Calcutta, or New York. They think they're window-shopping, and nobody knows or cares how long they look in each window. Or browsing in a bookstore. They have NO idea when* [cookies-type technology is] COOKIES ARE being used and someone is tracking them - who cares, and plans to make use, perhaps commercial use, of that information.,

One web developer told me: "Cookies aren't just okay, I think they're fabulous! Look, information isn't free. When you come to a web page, you are actually asking for information. In exchange, I want information about you. You better talk to me, and you better tell me the truth because this exchange is based on trust."

"Trust" is the word he used, by the way. He believes there is an implied agreement between the visitor and website owner. Consumers have a different perception altogether. Just as no one can

see them in their bathrobe, on the internet at 3 oclock inthe morning, they think no one can "see" them on any website. Perceptions are real, and very hard to change.

The web developer explains, "You're getting the information you want. I'm getting the information about you that I want." "Wait a minute, " I say. "I didn't know you were collecting data on me, you never told me that." "Well yes," he says, "It creates a database. Cookies are just a memory of a personalized relationship." Not if I don't know we're having one.

"Would you rather pay me \$5 or fill out a questionnaire?" he asks, to justify the "free exchange" of data that is taking place without my knowing it.

The problem is - at his and most other sites - we aren't given that choice. Some of us would actually rather pay, just to be left alone. Some of us would rather leave the site immediately, and not play the game. It's not a game, it's surveillance.

Technical people usually know how to turn off information-collection types of mechanisms. Can encryption shield the rest of us?

This type of technology has been around a long time. But when it's now embedded in browsers that most of the world is using - and consumers aren't told, aren't warned - we need to discuss disclosure. It's a social issue, again, not a technical one. But technology - encryption - can offer consumers protection.

The owner of the site, or browsers - ideally both - have an obligation to inform users: information is being gathered about you. Who's doing the collecting? And what are they doing with it? How might it potentially be used? If you're out there trolling for data, I believe I have a right to know I'm being watched. And the right to avoid your site. There must be full disclosure, both parties must have equal knowledge otherwise they're not really both parties to the contract. You can't be tricked into it, lured onto the site because it's cool. As the website's owner, you must be sure the person visiting your site understands what you're asking of them, so they can make a rational decision. "By the way, we use cookies" is not sufficient.

When the telco's implemented "Caller ID" they notified customers of the option to "block" your number, if you preferred, for privacy. Maybe encryption can do the same thing here - block our digital presence so we can move unnoticed around the web.

The same technical experts who say tracking is "not that big a deal" cannot agree on what cookies-type technology can - and cannot - do. This is scary for an everyday user: if the experts dont know for sure, why should ordinary folks be reassured it's "no big deal"?

I've been told conflicting information. With existing monitoring technologies today:

- Each site where the `{technology}` cookies are set knows only that you have been there ---