
Room for Debate: A Running Commentary on the News

« Room for Debate Home

« Back to Discussion

A 'Do Not Call' Registry for the Web?

Should there be a federal law making it harder to track consumers' behavior online?

The F.T.C. Should Stand Down

Updated December 2, 2010, 10:38 AM

Jim Harper is the director of information policy studies at the Cato Institute, the webmaster of WashingtonWatch.com and the author of "Identity Crisis: How Identification is Overused and Misunderstood."

In a May 2000 report, the Federal Trade Commission made an extravagant demand to impose blanket requirements of "notice, choice, access and security" across the online commerce landscape. Congress said: "No."

Much of the innovation in online consumer services since then occurred because the F.T.C. did not get the authority it wanted. The commission acknowledged the defects of the "notice-and-choice model" this week, making no apology for having been held in its thrall when the "Y2K bug" was a recent memory.

This latest report seems chastened by the diversity and creativity still emerging in the online world. But a federal agency cannot ever say, "there is nothing for us to do here."

So the commission has proposed to promote one technique to reduce some online tracking: a "do not track" system. The idea is to create a persistent setting in the Web browser that indicates a surfer's desire not to be tracked, then to back it up with surveillance and enforcement in hopes that the wishes expressed in this odd new protocol will become reality. (Does anyone remember the Can-Spam law? If wishes were horses)

There is a way to understand the currency of the "do not track" idea. Along with the F.T.C.'s need to always do something, technologists want to avoid an "arms race" in the privacy area. Widespread cookie controls would cause marketers to use Internet Protocol tracking, "Flash cookies," fingerprinting and other techniques to glean information about consumers.

But privacy advocacy is worse off in a public policy arms race. "Self-regulation" is the strange moniker given to agreements between industry and regulators, both content to divide up the business behavioral pie without actually responding to the desires of consumers. A "do not track" system would deceive consumers into believing their privacy is protected when they are actually only insulated from the rarefied discomfort of receiving accurately targeted marketing.

The social engineers at the commission should stand down. The Internet's real engineers should unite with consumers --- not government regulators --- to work on fuller, more genuine privacy protections.

Topics:

Widespread tracking controls would simply cause marketers to engage in an arms race, using other techniques to glean information about consumers.