THE WALL STREET JOURNAL.
WSJ.com

THE BUSINESS | Updated December 14, 2012, 10:11 a.m. ET

Are Digital Foxes Guarding the Web's Privacy Hen House?

By JOHN BUSSEY

If you want to see how industry self-regulation can fall short, take a look at the online advertising business and the fight over a do-not-track protocol to protect consumer privacy.

The Wall Street Journal

The Federal Trade Commission earlier this year asked industry to devise a self-regulated do-not-track solution—or risk government intervention.

It would seem to be in business's interest to keep customers happy—to give those who want it the guarantee that they aren't being tracked on the Internet. That's the idea behind a one-click, do-not-track button that would permanently block marketing firms that currently follow your activity from website to website.

The personal information they harvest—about your preferences, interests, vices, health-care research and even physical location—is used to pitch you products. Or it's sold for other uses.

Reacting to public concern about privacy online, the Federal Trade Commission earlier this year asked industry to devise a self-regulated do-not-track solution—or risk government intervention.

The public clearly wants something. A Pew Research study found 73% of respondents considered it an invasion of privacy if a search engine tracked their activity to personalize future search results.

And yet negotiations between advertising, marketing and privacy groups are stuck in a continuous loop. Email exchanged between members of the W3C Tracking Protection Working Group shows they still disagree over basic questions, such as what "do not track" should mean and how to assure compliance.

"We largely believe we've created do not track already," explains Linda Woolley, acting president of the Direct Marketing Association, a trade group. She says consumers can opt out by clicking online icons attached to certain ads and at industry websites such as aboutads.info.

Ms. Woolley cautions against getting too restrictive lest privacy advocates disrupt the essential beauty of the Internet: the free flow of free information. "The reason there's free content on the Web is because of advertising revenue," she says. What's more, ads that track preferences can save consumers time and money by pitching products they'll like. Many consumers value that.

"Smart firms won't go too far in invading consumer privacy because they realize—especially companies like Google and Facebook —that without the information consumers are giving them, they have no business at all," says Arun Sundararajan, of New York University's Stern School of Business. "This seems to be a situation where self-regulation is the way to go."

The problem is, self-regulation in the case of the Internet is often a contradiction in terms. Just this week, the FTC again slammed the industry, this time for tracking the actions of children online. Similarly, do-not-track buttons that do exist on browsers, such as on Microsoft's Explorer 10 (which is "on" by default) and Mozilla's Firefox, are ignored by many third-party marketers. And when the industry promises your data will be "anonymized," that promise comes with exceptions that test the definition of anonymous.

Current opt-out options are also problematic. Jeff Chester, a privacy advocate with the Center for Digital Democracy, says those opt-out icons and Web sites seem instead to encourage users to stay tracked. "They've created a self-regulatory system that doesn't undermine their objective of data collection."

Andrew King, of Dartmouth's Tuck business school, has studied self-regulation and says it has a sketchy record of success. It works best when there are clear rules, robust enforcement, and sanctioning of violators. That isn't evident in the current case, he says.

Which is one reason Sen. Jay Rockefeller introduced legislation last year that would require the FTC to create a do-not-track mechanism. I asked him if he thought the current deliberations would bear fruit.

"The industry's failure to follow through with its public pledge makes the case that self-regulation inadequately protects consumers and illustrates why strong federal legislation is warranted," he wrote back.

If the public is offered a comprehensive do-not-track option, what might happen?

In 2003, the government created the Do Not Call Registry, which allows consumers to opt out of telemarketing calls. Today, 218 million active phone numbers are registered. That isn't a perfect comparison to online tracking, but it gives a sense of consumer sentiment.

Jon Leibowitz, the head of the FTC, says he's still optimistic that companies will find a solution. There's general agreement on the big issues, he says. "What we're down to now is a few rogue advertising networks." Online advertising firms, he adds, know government regulation could be a worse result.

But it's unclear how potent that threat really is. Sen. Rockefeller's bill didn't get traction after he introduced it.

That may explain industry's strategy in the negotiations. Delay and rope-a-dope have worked so far. Maybe they will win the fight.

—Write to John Bussey at john.bussey@wsj.com; follow @johncbussey on Twitter

A version of this article appeared December 13, 2012, on page B1 in the U.S. edition of The Wall Street Journal, with the headline: Are Digital Foxes Guarding the Web's Privacy Hen House?.