All the Web privacy you want

December 14 2010, McClatchy-Tribune News Service

Microsoft announced last week that the next version of its Internet Explorer browser will include better privacy controls, giving users more protection against being tracked by advertisers online. Its initiative, which takes a novel approach to counteracting online tracking, illustrates why the government shouldn't rush to regulate in its zeal to address the problem. But it also highlights the scattershot nature of privacy protection, and the need for Washington to give people more say over how information about them is collected, used and shared.

The software giant's announcement came as federal officials are stepping up scrutiny of privacy practices in response to growing public concern. Privacy advocates have complained with increasing frequency about the amount of personal information being collected about Internet users, how often data are being shared without users' knowledge, and how aggressively some companies are translating supposedly anonymous information about Web users into profiles of real individuals.

The challenge for policymakers is that the Web is built around the collection and sharing of data. Much of that sharing is benign or even welcome. For example, frequent online shoppers may want their favorite retailers to store their credit-card numbers, or they may want to share their street address with shipping services. And people who watch videos on the Web may prefer to see commercials targeted to their location and interests over ads aimed at the undifferentiated masses.

But other surreptitious uses of data are not so innocent, such as when companies use browsing data to raise or lower the price of goods and

services a particular shopper is offered, or to develop profiles that combine supposedly anonymous online behavior with individuals' public records. Such actions are often made possible by the tracking "cookies" used by online advertising networks. These bits of software, which browsers download or update automatically when they reach a website displaying one of the network's ads, quietly record some of the actions the user of that browser takes online.

Microsoft's updated browser will offer users the option of blocking tracking cookies, advertisements and any other form of content from specific Web servers. The company won't suggest sites to block, but privacy groups are expected to supply lists that will be updated regularly. If enough consumers use the feature, it will put pressure on advertisers to abandon tracking in favor of less-intrusive means of targeting their pitches.

The initiative marks a shift for Microsoft, which had declined in the past to take aggressive measures against tracking software. Mozilla, maker of the Firefox browser, has also changed its thinking on the issue. Earlier this year it removed a proposed feature that would have killed tracking cookies not long after they were delivered, but it's now working on ways to give users more control over their privacy. There's been no similar movement yet from the other leading browser developers, but the actions by Microsoft and Mozilla show that the complaints about tracking have gotten loud enough to affect the market.

Naturally, online advertisers aren't entirely pleased with these developments, even as they scramble to respond to consumers' concerns by giving them better notification of tracking ads and a way to opt out of at least some of them. Their trade group, the Interactive Advertising Bureau, argues that encouraging people to block the kind of personalization that tracking enables will make it harder for sites to offer content and services for free, or at least charge those who block ads. But

Internet users should be the ones making that choice, rather than having it made for them on terms they don't like.

As welcome as the efforts by browser-makers may be, they address only the concerns related to ad networks' tracking cookies. Still missing are better mechanisms for limiting how personal information is collected and shared by websites and social networks, as well as the data brokers that aggregate information collected by others.

Today, online companies are required to do little more than publish a privacy policy that discloses what personal information they collect and share, and to honor that policy. The result has been a proliferation of privacy policies that are incomprehensibly dense and riddled with loopholes. What's worse, sites' policies don't bind the advertising networks that support them, which may be inundating people's computers with tracking software.

In a report last week, the FTC declared that the approach it has encouraged sites to take - notifying consumers about privacy policies and letting them opt out of practices they don't like - isn't working. The report outlined a good framework for approaching the issue, calling for all companies (not just those online) to give consumers a better view of how they collect and share personal information and a more effective means to control whether to provide that information.

The commission is still collecting feedback from the public on the details of its proposal, and it won't take formal action until next year. Even if it moves ahead with the report's suggestions, though, it's not clear what authority the FTC has to enforce them. So far, its power has been limited to cracking down on sites that don't honor their own privacy policies.

Existing federal law protects only certain types of personal information

against improper use or disclosure, including medical records and credit reports. Considering how much information is routinely collected and shared online, and how that information can be used to favor some consumers and disadvantage others, Congress needs to provide more protection.

The solution isn't a special set of rules for the Web, but rather some basic, enforceable principles for personal information privacy. At least four are worth enshrining into law. First, businesses should disclose what forms of personal information they're collecting and sharing, especially when they're doing it behind the scenes. Second, those disclosures should be timely and easy to understand. Third, consumers should be able to choose not to have personal data shared in ways that aren't commonly accepted or that go beyond the limits imposed when the information was initially collected. And fourth, consumers should have the right to correct errors in the information that's compiled about them if it's put to commercial use.

The point is to let companies innovate with technologies and business models while making sure the public is an informed and willing participant. Given the tradeoffs involved, many Internet users may choose to let sites collect and share just as much personal information as they do today. But it should be their choice.

More information: This editorial appeared in the Los Angeles Times on Monday, Dec. 13.