New Jersey Law Journal

VOL. 206 - NO 11 DECEMBER 12, 2011 ESTABLISHED 1878

COMMENTARY

Open the Black Box (or, at Least Respect Consumer Preferences)

BY GRAYSON BARBER

When you visit popular websites, you are being tracked by a number of services that place invisible embedded content on your laptop or take information from it.

For example, an advertising network may, in addition to delivering ads, surreptitiously obtain information about you and sell it to third parties.

A salacious example is "YouPorn," which was caught in 2010 extracting the Internet search histories of every laptop that connected to its YouTube-like service. Visitors to YouPorn might have thought they were anonymous, but every morsel of data that could be extracted about them was being taken surreptitiously.

Many people perceive such third-party tracking as an invasion of privacy. In *State v. Reid*, 194 N.J. 386 (2008), the New Jersey Supreme Court noted in dicta that people have a reasonable expectation of privacy when they are trying to surf the web anonymously. The Federal Trade Commission, asserting its consumer protection jurisdiction, agrees that our expectations count for something.

The rejoinder from the Big Data industry is that an implicit agreement exists every time you visit a website. In exchange for free content and services, you agree to surveillance of your online behavior. The FTC's response is simple: give consumers a chance to express their preferences, and see whether online vendors will respect those preferences.

The FTC's "Do Not Track" initiative would give consumers a chance to say no to online tracking. The "DNT" label evokes the FTC's most popular initiative (and possibly the most popular government initiatives of all time), the "Do Not Call" registry, which allows consumers to stop telemarketers from contacting them by phone.

"Do Not Track" adds a little piece of computer code to the message your laptop first transmits (the HTTP header) to every website you visit. HTTP headers say in effect, "I do not want information about me to be redisclosed." It would allow contextual ads but not behavioral advertising; if you visit NYTimes.com, you will receive ads from *The New York Times*, but not from hidden, third-party companies.

As of today, vanity searches cannot help you track your digital reputation. Sucking your data into a black box for purposes you cannot discern, data companies treat you as a commodity. You are not a client of Facebook; to the contrary, you are a source of data that will be sold to the companies that are paying Facebook for your personal information.

The Network Advertising Initiative, a self-regulatory group, says that mandating this kind of low-cost opt-out will kill the business model that funds the web. According to the Stanford Center for Internet and Society, half of NAI members do not honor requests from consumers to remove their tracking cookies.

But a measure of trust is essential for business to be conducted on the web. Microsoft says it is eager to get online privacy right, its incentive being its big financial stake in getting users to trust the Internet cloud. To that end, Microsoft Tracking Protection (for Internet Explorer 9) allows users to block third-party cookies, tracking pixels, web beacons, hit counters, analytics scripts and other tools.

This makes sense. Data collection and use is much more extensive than was anticipated even a few years ago. In an increasingly opaque way, companies transfer user information to third parties. And now, there is growing concern that companies are manipulating their privacy policies and settings to confuse and frustrate users so that more personal information will be disclosed. The European Union, in another example, plans to give consumers more control over online tracking.

People should be able to learn how their personal data is being gathered and register their objections if they feel the information is being mishandled. To find out how to install "Do Not Track" on Internet Explorer, Firefox and Safari, visit http://www.DoNotTrack.us (Stanford Security Lab). For a list of businesses honoring Do Not Track, visit http://www.donottrack.us/implementations. ■

Barber, a solo in Princeton, concentrates on privacy issues.