
Keeping Up with the FTC's Thoughts on Notice, Choice and Persistent Identifiers

APRIL 22, 2016

With advances in cross-device technologies and the ever-growing Internet of Things, what should the online advertising industry be doing to address consumer concerns about online tracking? "Offer them easy-to-use tools to block all of the techniques used to track them," answers Jessica Rich, Director of the FTC's Bureau of Consumer Protection. Recapping her Q&A Session with Leigh Freund at last week's [Network Advertising Initiative \(NAI\) summit](#), Rich today [shared her thoughts](#) on the state of the online advertising industry.

In addition to calling for easier tools to block tracking technologies, she called for industry to do more to better inform consumers about how they can be tracked online and on their devices. While applauding efforts by the NAI and the Digital Advertising Alliance (DAA) to provide tools to control targeted advertising and address cross-device tracking, she suggested more is needed to keep up with rapid technological changes in online advertising. Disclosures—and privacy policies—should address not just cookies, fingerprinting and cookie syncing, but any proprietary technologies that combine these tools, she said.

Director Rich cautioned companies against leading consumers "to believe tracking is more limited than it is." If a company offers choices that do not actually cover all the mechanisms used to track consumers, this should be clearly and prominently disclosed. Failure to do this, she noted, is likely deceptive under the FTC Act.

She also reiterated the FTC staff's position dating back to its [2009 Online Behavioral Advertising Staff Report](#) that the FTC staff regards "data as 'personally identifiable,' and thus warranting privacy protections, when it can be reasonably linked to a particular person, computer or device. In many cases, persistent identifiers such as device identifiers, MAC addresses, static IP addresses, or cookies meet this test." She went on to say that "If you're collecting persistent identifiers, be careful about making blanket statements to people assuring them that you don't collect any personal information or that the data you collect is anonymous. And as you assess the risks to the data you collect, consider all your data, not just the data associated with a person's name or email address. Certainly, all forms of personal information don't need the same level of protection, but you'll want to provide protections that are appropriate to the risks."

Beyond her regulatory stick, however, Rich also offered building consumer trust as an important carrot for the online advertising industry. She suggested that the rise of ad blockers and other consumer efforts to limit information sharing reflect a lack of “simple, easy-to-use and comprehensive” choices when it comes to online tracking.