FTC Updates Consumer Guidance for Online Tracking

Alyssa Z. Hutnik

June 24, 2016

On June 23, the FTC updated its consumer information page to provide updated guidance on "Online Tracking." The updated guidance is intended to provide consumers with information on different methods of tracking, how they work, and how consumers can control such tracking. While directed to consumers, updates to this page can also help businesses understand how these online tracking technologies work, and identify what the FTC expects businesses to do.

The previous guidance, titled "Cookies: Leaving a Trail on the Web" (last updated in November 2011), primarily addressed cookies (including first-party cookies, third-party cookies, and flash cookies), provided consumers with general information on how to control cookies, identified how consumers can opt-out of receiving targeted ads, provided a brief overview of "Do Not Track," and identified that new technologies were constantly emerging.

The updated guidance document updates and expands upon this information to address new forms of online tracking (*e.g.*, device fingerprinting, cross-device tracking), new tracking technologies (*e.g.*, use of unique device identifiers or HTML 5 cookies), how tracking in mobile apps occurs, and how consumers can generally limit or block tracking online, in apps, or across devices.

So what is the big-picture takeaway for businesses? Consumers may not fully understand online tracking, including their options for minimizing or preventing such tracking from occurring. Businesses can help educate consumers concerning their online tracking by providing clearly identifiable ways in which consumers can review information about the company's collection, use, and disclosure practices, and ways to limit cookies and other tracking technology. This may include a clearly written privacy policy or other consumer facing document, or in the device settings as suggested by the FTC. Lessons learned from past FTC enforcement actions (including the FTC's action announced yesterday against InMobi) also illustrate the risks associated with business practices that appear to circumvent a user's privacy decisions or a device's privacy settings.