Hughes Hubbard & Reed

Device Fingerprinting and Targeted Marketing: The Next Digital Privacy Battleground?

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

In one of the latest advances in what has been called "a technological arms race between tracking companies and people who seek not to be monitored," device fingerprinting, a technology originally developed to prevent software piracy and credit card fraud, appears set to become a powerful new tool for online marketers. But recent calls to increase consumer control of personal information will likely impact how device fingerprinting technologies are integrated into marketing efforts and may slow its widespread adoption. What exactly is "device fingerprinting"? Every time a computer or other mobile device connects to the Internet, it broadcasts information about its properties and settings (such as which browser is running, screen resolution, speed of connection, etc.) in order to interact smoothly with websites and other computers. Device fingerprinting technology collects this information to build a profile that can identify the individual computer or device, and in some instances, the person using it. Before its adoption for online marketing, fingerprinting technology was primarily used to prevent software theft, providing a means to confirm that the subject application was only used on authorized computers. Anti-fraud companies use the technology to identify devices that had engaged in fraudulent transactions to help them prevent similar occurrences in the future. Privacy legislation proposed this July even advocated its use to identify consumers who had opted-out of online tracking. But device fingerprinting could also allow for much more effective tracking of online behavior than other current technologies. Where cookies can be blocked or deleted, it's much more difficult to prevent fingerprinting or to delete a fingerprint after it has been collected. One study, surveying 70 million website visits, found that a fingerprint of an applicable device could be generated 89% of the time whereas cookies could only be used 78% of the time. One developer of device fingerprinting technology claims that it is even able to link the fingerprints of different devices that appear to be used by the same person. Eventually, the company plans on adding offline activity to the individual's profile, using email addresses and names the user entered while browsing the web to pull information from other databases.

By collecting, generating and selling this information to marketers, the device fingerprinting could become the basis to deliver targeted ads based on a consumer's activity from their computer, mobile phone and other devices. Fingerprinting and other forms of digital tracking are currently legal but both federal regulators and

several members of Congress have warned that the government will intervene if the online-advertising industry does not start doing more to protect consumer privacy. Recently, the FTC recommended that a Do Not Track System be implemented if the industry doesn't start coming up with its own solutions soon. The FTC proposal would require web browsers to implement a do-not-track setting directly in the browser to enable end users to block web service providers, marketers and advertisers from monitoring their online behavior. The FTC would then police companies that implement tracking technologies and tools to ensure that they comply with user requests. The ad industry's current opt-out system only allows consumers to opt-out of targeted advertising, not tracking altogether. The industry has taken notice. Some marketing firms say that they will create an opt-out function if they adopt fingerprint technology, though the details of how that would work are still unclear. Other initiatives include the "Open Data Partnership", a service that would allow consumers to see what information has been collected about them, and opt out of being tracked by participating firms. The service is intended to be a response to the government request for more transparency and consumer control. Eight data and tracking firms have already committed for the service's launch in January. Microsoft has also revealed plans for a tool to block tracking in its next version of Internet Explorer. The tool, once enabled, will allow users to block tracking attempts from specified web addresses used by tracking companies. But in order to use the tool, users have to direct the browser as to which tracking attempts should be blocked by selecting from lists compiled by privacy groups and other outsiders. There won't be any default setting to block all tracking attempts. Additionally, the tool will only block tracking by certain technologies, such as cookies and beacons. It doesn't address new technologies like digital fingerprinting and "deep packet inspection," a form of monitoring which analyzes data as it travels from the internet to the computer. While support for consumer protections are gaining ground, the $23 billion online advertising industry warns that an end to tracking could also mean an end to the free web content that is currently subsidized and supported by targeted advertising. And some members ofCongress have expressed hesitation about any legislation that might hurt economic recovery. Data tracking has also enabled the customized web experience that many consumers have come to rely on. In order for any solution to be viable in the long-term, it will have to find some way to balance these competing concerns. In the coming months, we will continue to monitor this and other developments in the ongoing debate over privacy on the internet.

Related Areas of Focus

Media, Technology & Commercial Transactions