App Tracking

Consumers want more control over their personal data but often fail to adopt available safeguards. A new privacy feature in the iOS mobile operating system portends to paint a different picture. A native prompt in the iOS mobile operating system now requires consumers to grant or deny apps permission to track them. To examine how consumers respond to this App Tracking Transparency policy, we use device-level location data from more than 7 million iOS and Android devices. We focus on two questions: (1) does the amount of tracking data consumers emit through their devices decrease after the policy change and (2) among which consumers is the data reduction most prevalent. For a location data provider collecting data through multiple apps, we find the frequency of data collection from iOS devices decreases following the policy change. This reduction is driven by devices becoming unobserved and by observed devices emitting fewer pings, suggesting some consumers uniformly deny tracking requests while others selectively deny them. The data reduction is more pronounced among consumers who visit privacy-sensitive locations, implying consumers who may want to mask their behaviors take steps to do so. The reduction in data is also greater among consumers who visit locations associated with a data breach, suggesting consumers whose trust in firms has eroded adopt protective measures. We confirm these findings by showing robustness to sensitivity analyses, different matching specifications and placebo tests. These findings have implications for data brokers, digital advertisers, retailers and policymakers.