Hughes Hubbard & Reed

California AG's "Recommendations" Suggest New Standards for Privacy Protection in Apps

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

California's attorney general recently released a set of privacy practice recommendations for app developers . The recommendations, which the California AG acknowledged offer greater protection than existing privacy law, are not legally binding. However, since the AG is charged with enforcing the California Online Privacy Protection Act (OPPA), the recommendations provide insight into how that law may be interpreted in connection with privacy investigations and enforcement actions. And since any app that collects data from California users must comply with the requirements of OPPA, the scope of that law is broad and, like the federal Children's Online Privacy Protection Act, which we recently analyzed, these recommendations could have far-reaching effects that must be seriously considered.

Passed into law by the state legislature in 2003, OPPA requires a "conspicuously post[ed]" privacy policy in any app collecting "personally identifiable information" from consumers. The policy must identify what information will be collected, explain how users can edit personal information, describe how users are notified of privacy policy changes, and identify the policy's effective date. The California AG commenced a suit against Delta Airlines in 2012 alleging that Delta failed to properly clarify what personal information it collects and what it does with that information. A second lawsuit against another developer is expected in the coming months.

The new recommendations were targeted at a variety of parties, but app developers were the primary focus. The California AG suggested developers (1) use a data checklist to review what personally identifiable data an app could collect and use it to make decisions on privacy practices, (2) not collect any personally identifiable data not needed for an app's basic functionality, (3) develop a clear and accessible privacy policy, and (4) use special notices or detailed privacy controls to identify collected data not needed for basic app functionality.

Mobile ad networks and app platform providers also received a fair amount of guidance. Ad networks were encouraged to avoid out-of-app ads, provide a privacy policy to app developers to enable targeted ad delivery through the network, and move away from unchangeable device-specific identifiers and transition to app-specific or temporary device identifiers. Platform providers were instructed to make privacy policies accessible from the app platform so a user could review them before downloading any apps and to generally use the platform to educate users on mobile privacy.

Finally, the California AG made limited recommendations to operating system developers and mobile carriers. Operating system developers should create global privacy settings to allow users to control the data and device features accessible to apps, while mobile carriers ought to leverage their customer relationships to educate on mobile privacy.

These new recommendations force virtually any company in the "app space" to reconsider their privacy and data collection practices and consider whether or not those policies comply with the California AG's views on how privacy policies should be scoped and implemented. Since nearly all mobile apps can be accessed and used by California users, any developer whose app collects information from users should take notice.

Related Areas of Focus

Media, Technology & Commercial Transactions