

Privacy a major challenge for mobile video

Mobile device applications (“apps”) have come a long way in just a few years, and the app industry’s growth has been nothing short of staggering. There are now more than a million apps available for consumers, and more than 1 billion apps were downloaded worldwide during the last week of 2011 alone. As a reflection of this growth, smartphones are now outselling traditional personal computers. Smart phones and tablets will form a key part of tomorrow’s television ecosystem. While not necessarily replacing the main television, smart phones and tablets will become the connected “Second Screen”.

Despite the growth of the app ecosystem, media reports in recent months have highlighted a number of concerns over how many apps use their users’ personal information, including sharing the information with third parties. Some apps are reportedly sharing address book contents, photo libraries, precise location information, and other information without specific permission from users. Although several recent industry efforts – such as an agreement with the California Attorney General, new guidelines from GSMA, and a template app privacy policy from The Mobile Marketing Association (“MMA”) – will help address some user concerns, new challenges lie ahead. Specifically, as wireless providers deploy 4G networks and mobile TV services and a variety of companies attempt to turn mobile devices into the new “second screen” for video content, all members of the app ecosystem will need to remain vigilant in addressing data privacy and security issues under a fast-evolving regulatory landscape.

California agreement

In February, six leading mobile app platform operators – Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research in Motion – agreed to a “Joint Statement of Principles” with the Attorney General of California. The agreement was announced after a series of recent headlines raising questions about the sufficiency of current app privacy practices, and is designed to promote transparency and consumer control over personal data, as well as compliance with existing privacy laws. It also effectively creates enforceable, nationwide mobile app privacy standards.

“By ensuring that mobile apps have privacy policies, we create more transparency and give mobile users more informed control over who accesses their personal information and how it is used,” Attorney General Harris stated.

To promote transparency, the six app platform operators agreed to include, as part of their app submission process, optional fields for app developers to describe an app’s privacy practices or provide a link to a privacy policy. When developers provide this information, the platform operators agreed to make it available to consumers in their app store. As a result, consumers (and privacy advocates) will now be able to learn about an app’s privacy practices before downloading and installing the app. In addition, they will be able to compare the stated policies against actual practices for compliance with the California act and other existing laws.

Under the agreement, the platform operators will also provide a mechanism for app store users to report apps that do not comply with applicable laws or terms of service. They will also develop a process for addressing such non-compliance, facilitating a self-regulatory enforcement regime to help promote improved privacy practices.

Finally, the platform operators agreed to continue collaborating with the Attorney General on mobile privacy best practices. The parties are scheduled to meet again with six months to evaluate the state of mobile privacy.

GSMA guidelines and MMA privacy policy

Privacy enhancements are also occurring globally. Earlier this week at the Mobile World Congress in Barcelona, the GSMA published global privacy guidelines for mobile apps. The guidelines are intended to improve user trust and confidence through increased transparency and consumer choice. Leading mobile carriers in Europe are starting to implement the guidelines on their own branded apps, and others are expected to follow their lead.

"...viewing habits could prove even more valuable for advertisers when combined with a user's location"

"...advertisers will be keenly interested in the multitasking activities that users are engaging in while watching television"

The MMA also released a template mobile app privacy policy earlier this year. The template is designed to address key privacy issues that arise under many mobile apps.

Mobile data privacy and security issues on the horizon

The deployment of 4G wireless networks will enable a host of innovative new streaming video services and, with them, new data privacy and security issues that will need to be addressed. For example, content and service providers will have access to additional information about users' viewing habits, which could spur new targeted advertising models and social network platforms. In addition, these viewing habits could prove even more valuable for advertisers when combined with a user's location. Moreover, to the extent mobile devices increasingly become the "second screen" used to supplement traditional at-home television viewing, content and service providers – and advertisers – will be keenly interested in the multitasking activities that users are engaging in while watching television. In light of these looming issues, carriers, equipment manufacturers, content providers, app developers, app store owners, and other members of the mobile app ecosystem should continue educating themselves about the importance of protecting users' privacy and data security, and they should continue to monitor developments in this area.



Mark Brennan

T +1 202 637 6409

mark.brennan@hoganlovells.com
