
Pokémon Go Presents Confidentiality, Trade Secret and Privilege Concerns for Users Who Also Use Google Accounts for Business Purposes

By Elizabeth F. Collura / Jul 13, 2016

The newest, hottest game, Pokémon Go, has already been downloaded over 7.5 million times on iOS and Android phones since being released less than a week ago. The free-to-download game is bringing in \$1.6 million in daily revenue in Apple's iOS store alone, based on in-app purchases. This augmented reality game is currently on the fast track to overtake social media apps in terms of amount of active users.

In the early days of the game's release, for users playing the game using a Google account login, the game's standard terms and conditions gives the developer (Niantic) unfettered access to Google Drive. Such access makes device owners' confidential information vulnerable. Those standard terms grant Niantic read and write permissions for documents stored on the user's Google Drive, as well as access to Gmail and contact lists. The permissions also authorize Niantic to sell the information obtained through the accounts.

Niantic has publicly stated that they are working to limit the scope of these permissions, and that it is not Niantic's intent to gain full access to users' Google accounts. However, the potential to broadly reach confidential information through an exciting game offering should remind businesses of the importance of reviewing internal confidentiality protocols and protecting confidential information.

Businesses must be vigilant to protect confidential information, especially those businesses allowing employees to "BYO" electronic devices for work purposes or who allow employees to use work-issued devices for personal reasons. Broad permissions, such as those in the standard terms for Pokémon Go game, raise questions for:

- Businesses who use Google Drive to store or any Google account to access their confidential, proprietary or trade secret information.
- Businesses who use Gmail or Google Drive to communicate with their attorneys, and attorneys using Gmail or Google Drive or any other Google account for client-related reasons. The game's standard terms may raise an argument that, by granting Niantic access to the Google accounts, any applicable privilege under the attorney-client privilege or work product protection has been waived.
- Businesses in the healthcare field using Google Apps as their HIPAA compliant records platform. At this stage it is unclear how the broad access terms of the game interact with the protections of Google Apps accounts, and whether the game's permissions "open a door" to a HIPAA violation.
- Any other business who handles information made confidential or protected by law, who stores confidential information in a Google account or uses any Google account for business purposes.

To protect against potential compromise of confidentiality, business best practices include:

- Having a comprehensive policy in place for employees' use of technology, designed to minimize the risk of compromising confidentiality.
- Limiting employee use of business-related Google accounts to business purposes only. One easy approach for the Pokémon Go game is for players to create a dedicated Google account solely for playing the game.
- At a minimum, players should revoke Niantic's access to all Google accounts through the game. This is accomplished by: (1) Within your Google account, launch the Google security page; (2) Select Pokémon Go and click "Remove" to revoke full access.

Clark Hill attorneys and professionals have a depth of experience in dealing with potential confidentiality, trade secret and privilege concerns, making our firm an ideal resource for evaluating your business's risks and needs. Since 1890, clients have received an unparalleled level of service that is thorough and appropriately focused.

For questions regarding this e-alert, contact Elizabeth F. Collura at (412) 394-2328 | ecollura@clarkhill.com or another member of Clark Hill's Litigation Practice Group.