Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

'Pokemon Go' Developer Wades Into Privacy Minefield

By **Allison Grande**

Law360, New York (July 13, 2016, 11:20 PM ET) -- The rapid rise of the hit smartphone game "Pokemon Go" has opened the developer of the app up to heavy scrutiny from regulators and users, who may end up wielding a variety of privacy and consumer protection laws to address concerns over the type and quantity of data being collected.

Although it is barely a week old, the augmented-reality app has taken the smartphone world by storm, having been downloaded nearly 10 million times in the U.S., sending the stock of collaborator Nintendo soaring while in the process drawing sharp criticism and inquiries from privacy advocates concerned with what kinds of data the app is amassing from its wealth of users. Niantic Inc., which was founded in 2010 as an internal startup at Google Inc., developed the game in collaboration with Nintendo and The Pokemon Co.

The most high-profile scrutiny to date has come from Sen. Al Franken, D-Minn., who on Tuesday sent a letter to Niantic expressing reservations about the app's collection of personal data, although a bevy of other notable commentators — including the news satire site The Onion — have also weighed in.

"Any time The Onion's lead FAQ on your product is: 'Q: What is the object of Pokemon Go? A: To collect as much personal data for Nintendo as possible,' Al Franken is the least of your worries," Sheppard Mullin Richter & Hampton LLP privacy and data security group co-chair Craig Cardon said.

The heightened attention being paid to the app's potential privacy pitfalls is largely a function of the popularity it has amassed in its short life, which has significantly raised the profile of already common issues such as the overcollection of consumer data and the protection of children's information.

"The amount of publicity it has gotten in the past few days operates as a lure for regulators and lawmakers because they're hearing about it from everywhere," Foley Hoag LLP attorney Erik Schulwolf said.

The main issue that will likely be top of mind for both regulators and the app's users themselves is what information the developer is collecting, using and sharing — and whether those practices match up with what it has told users to expect.

"The 'Pokemon Go' privacy controversy demonstrates that even with good notice and choice, consumers and regulators have concerns about data collection and use that may be unexpected or beyond what is necessary to support functionality and the business model," BakerHostetler partner Alan Friel said.

Franken homed in on these concerns in his letter, asking Niantic for more information about what data is being collected from users' phones and how it's being used. The senator expressed specific concerns about the app's collection and use of geolocation data, as well as reports that the app received full access to the profiles of users who signed in with their Google accounts.

While attorneys who reviewed the app's privacy policy told Law360 Wednesday that the disclosures appear to be comprehensive and clearly lay out how and what data is being collected from both children and adults, the question of whether the app's actual data collection practices match up with these representations is likely to be a topic of interest for both the Federal Trade Commission and the plaintiffs' bar.

"While the privacy disclosures and policy are consistent with what one may normally see in the industry, they will get much greater scrutiny because of the scale and velocity of growth of the app," Cardon said. "Users are both voters and class members, and dollars are potential damages. Therefore, regulators and plaintiff's class action lawyers have to look at the privacy issues surrounding 'Pokemon Go.'"

If it comes to light that the app's data collection policies and executions do not sync, consumers are likely to turn to state consumer protection and unfair competition laws to assert they were not told about the full extent to which data was being collected from them, and the FTC has Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices, at its disposal.

"You can have the most comprehensive privacy policy, but the devil is always in the details, and it's important for any company that collects personal information to make sure that what they are communicating to its user base is what it's doing," Shook Hardy & Bacon LLP attorney Eric Boos said, adding that compliance with the FTC Act is especially important because the regulator in recent years "has shown that it is the leading government regulator when it comes to these issues" and won't hesitate to take a deep dive into these topics and take action if necessary.

One recent case announced by the FTC last month is particularly pertinent to the "Pokemon Go" saga. In that action, the FTC hit Singapore-based mobile advertising company InMobi with a $4 million civil penalty — which was suspended to $950,000 based on the company's financial condition — to resolve claims that it tracked hundreds of millions of consumers' locations without permission in order to serve them geotargeted advertising.

"U.S. regulators are increasingly discussing location, particularly precise location, as highly sensitive data that should justify heightened notice and choice," Friel said.

The InMobi action also notably involved allegations of privacy violations tied to the collection of children's data. The FTC asserted that the company ran afoul of the Children's Online Privacy Protection Act by scooping up information from apps that were clearly directed at children without ever obtaining permission from parents.

As with InMobi, the developers of "Pokemon Go" are likely also going to face questions about their collection of personal information, including geolocation data from children under 13, given the subject matter and content of the gane.

"Even though the app seems to be popular with an older generation, at the end of the day, it's hard to escape the fact that it's aimed at children, and any time that children are involved, that really raises red flags and gets people involved," Boos said.

Phyllis Marcus, a Hunton & Williams LLP counsel and former FTC advertising practices division chief of staff, said that the app's written privacy policy that she was able to review appeared to "be relatively clear and follow the requirements of COPPA," although she did say Franken's letter raised questions about potential statutory violations that are not usually widely addressed, including whether the app collected more data from children than was reasonably necessary to play the game.

"So arguably, if the app is collecting more information than it needs to do to make the game go, the developers could be in violation of the COPPA data minimization provisions," Marcus said.

However, she did note that Niantic is likely to gain brownie points for not ignoring the fact that kids under 13 are using its app and setting up procedures to identify these users and gain their parents' consent, and for making changes to their privacy policy in recent days that limits the type of information the developer can access from Google users.

Aside from the allegations that it may have collected too much information, Niantic could also find itself in hot water if hackers find their way to the treasure trove of data that the app has collected from its millions of users, attorneys said.

"Its privacy policy allows Niantic to collect fairly extensive information, which obviously creates a concern not necessarily because of any untrustworthiness on the part of Niantic, but due to the concerns that hackers might be able to get their hands on this information," Schulwolf said.

Even if nefarious actors don't get into the system, users that are uncomfortable with the data that the app sweeps up have plenty of other potential avenues to turn to for relief. One possible route is to sue under the Computer Fraud and Abuse Act, which prohibits businesses and others from exceeding their authorized access to a system, according to Weisbrod Matteis & Copley PLLC partner Peter Toren.

"There's no doubt that a smartphone would meet the definition of a computer under the CFAA, and to the extent that the developer is obtaining information on a person's mobile device that they are not authorized to obtain, that seems as though it would constitute a violation of the CFAA," Toren said.

The federal Video Privacy Protection Act and Michigan's Video Rental Privacy Act could also be used against the developer. While plaintiffs have recently faced several setbacks in trying to expand the statutes beyond brick-and-mortar video stores, augmented reality may offer a new frontier for consumers to attempt to crack, Troutman Sanders LLP partner Mark Mao said.

"Although Congress clearly did not have [augmented reality] in mind when it passed the VPPA, such opportunities are open for plaintiffs when old laws meet new and unanticipated technologies," Mao said. "AR may be the next frontier of video-data litigation, as the dust settles on issues relating to what constitutes ‘personally identifiable information’ and who are ‘subscribers.’"

Finally, components of the game such as the "lure" and "gym" features that encourage users to congregate at a certain location to catch Pokemon could additionally open Niantic up to third-party liability if someone is injured or accused of trespassing, attorneys say.

Given the wide range of liability that could be at hand, developers eager to follow in “Pokemon Go”'s highly profitable footsteps would be wise to carefully consider what types of data they are collecting, and why, in order to avoid class action and regulatory backlash down the line.

"With any kind of app developer we work with, it's important to run through some beta testing before they roll things out to the general public, because no matter how good their policies are, there's always going to be a little something that they don't think about," said Colin Zick, co-chair of Foley Hoag's privacy and data security practice. "While app developers do generally have a tight timeline with limited money, taking the time to work all the bugs out can actually help the app in the long term and help avoid the wrath of law enforcement and regulators."

--Editing by Philip Shea and Brian Baresch.
