Mr. John Hanke, CEO
Niantic, Inc.
2 Bryant Street, Suite 220
San Francisco, CA 94105

Dear Mr. Hanke:

Pokemon GO is arguably already the most popular mobile game in history. It has been downloaded over 20 million times and boasts a daily population of more active users than Twitter. Because many of the users are children, we are writing to express our strong concern that far greater attention must be paid to the impact of Pokémon GO on their privacy, security, and safety.

The game is fast on track to be a billion-dollar business in its first year. Recent headlines tout its revenue potential, with some estimates placing daily revenue from in-app purchases alone at over $2 million. Even investor Nintendo has seen a 30% increase in its market capitalization – to more than $30 billion – just since last Wednesday. Experts estimate as much as half of the game's revenue could come from advertising – including with sponsored locations, reportedly launching today in Japan.

Niantic has created an exciting, active game – one that, as our 3-out-of-5-star review notes – is nonetheless marred by "various security and safety issues." These issues are so significant that it appears that, during the game's development, the desire to score a big and lucrative hit outweighed considerations of the privacy, security, and physical safety of users, in particular the many users who are children.

Common Sense Media and our advocacy platform Common Sense Kids Action are committed to helping all children and their parents thrive in a rapidly changing world of media and technology. We provide advice to tens of millions of parents and hundreds of thousands of teachers about the wise use of media and technology, at home and in school. And we encourage policymakers and businesses to act in the best interest of children when designing public policy or developing new technology. It is in this context that we write to express significant concerns about the risk to children's privacy, security, and safety posed by Pokémon Go. These concerns include:

Developers appear to have paid scant attention to privacy and security.

When the game was initially released, the iOS version requested full permission to a user's Google account, allowing it to see and modify essentially all information in the account, including Gmail and documents stored in Google Drive. These permissions are completely out of proportion with anything needed to play the game. Following widespread criticism, Niantic claimed the game was "erroneously requesting" access and adjusted the game's setting. This is an enormous red flag about a lack of quality assurance on the game overall. Some technology experts have referred to it as the likely "result of epic carelessness," which gives us pause as we consider other privacy and security implications of the game.

Developers did not consider the game's physical danger for children and others.

In addition to our concerns about user privacy and data security, we have equal if not greater concerns about the potential for significant physical harm to befall game players. Children, in particular, are more likely to have difficulty identifying when game play may pose a real life threat to their safety. Since the app was released earlier this month, users and those around them have come into real danger while playing. Distracted players have broken bones, gotten into car accidents, and two even walked off of a cliff. In some instances, children have been sent to inaccurately depicted locations, including private residences (and at least one resident responded with shots fired at players, including a minor). Stops have included a home for sex offenders and a location with large numbers of drug addicts. Firehouses and other public safety providers, intentionally programmed as locations into the game, have been distracted from providing critical services as they attempt to manage Pokemon hunters.[1] Police departments and public transit have started warning citizens about the game. Worse, criminals have used stops as lures to commit acts of robbery or violence against unsuspecting and distracted players.

In light of these very real and serious concerns, developers must do better with Pokémon GO and future products. Pokémon GO must take the necessary steps to ensure users, particularly children, are not placed in harm's way in the digital or physical world. As Niantic makes continued updates to the game and introduces new products, we urge Niantic to ensure the privacy, security, and physical safety of Pokemon GO users – particularly the millions of child players, by doing the following:

- **Obtain informed and meaningful consent from parents**: Parents must be the ones who decide which games their children play and what is an acceptable use of their data – decisions parents cannot make when privacy policies are vague and business models profit off players in multiple, and often opaque, ways, such as via confusing in-app purchases and targeted ads seamlessly incorporated into a game.

[1] Further, places of memoriam, such as the Arlington National Cemetery and the Holocaust Museum have had to issue statements asking users not to catch Pokemon on their properties out of respect for the deceased.

Niantic, and other app developers, need to make it easy for parents to understand what apps do, how game play works, and how data is collected and shared.

As such, we urge you to:

- Provide clearer and more conspicuous warnings about the dangers of gameplay in an augmented reality environment, including warnings to parents who consent to gameplay on behalf of their children.
- Provide specific information regarding information sharing, including
  - the process and standard by which user data is de-identified;
  - the purposes for which user data would be shared or sold, and;
  - a list of companies as well as "third party service providers" to whom Pokemon GO shares, sells, or otherwise makes available user data.
- Enable users, particularly parents acting on behalf of their kids, to easily opt-out of information sharing that is not integral to the game. For example, the Children's Online Privacy Protection Act (COPPA) requires that parents have the option to prevent sharing of their children's personal information with third parties. This is an essential protection for children, who should not have a marketing profile built on them as the price of playing a game.
- Be fully transparent with parents and kids about commercialization in the game, including in-app purchases, targeted advertisements, and sponsors. It can be particularly confusing for kids – and frustrating for parents – when games don't clearly distinguish in-app play money from real dollar purchases. And kids, who may be playing without supervision or may not understand the commercial nature of the message, are especially vulnerable to personalized ads in a setting like Pokemon GO. Pokemon GO should clearly explain any use of targeted advertisements and identify physical locations, brands and companies who have paid, or provided other consideration, to be included as a part of gameplay.
- Provide parents with controls over in app advertising, and the ability to opt out of targeted advertising.

- **Take specific precautions to protect children's physical safety:** When apps collect and share sensitive information, such as geolocation, or when they allow users to interact with one another, developers must be careful. This is especially true when the apps target or appeal to kids. It is the responsibility of Niantic to take extra precautions to provide for the safety of its users, and the people around them, as it directs them to real world locations. Children, in particular, are likely to have a false sense of security while using the app, often lacking the maturity and judgment to understand when gameplay poses a real life threat.

  As such, we urge you to:

- Ensure that the geolocation information of users remains private and secure, and provide clear mechanisms for users to control when and if their location is tracked or shared.
- Proactively address and swiftly respond to eliminate real world locations from game play that have been demonstrated as a safety or security threat, or that a reasonable person could identify as a safety or security threat.
- Allow parents to turn off functionality that sends their children to lures or other locations added by other players, and considering providing clear visual indications of when lures have been dropped in specific locations.

- **Ensure privacy and security from the ground up:** That Pokémon GO originally and erroneously requested full permission to a user's Google account as a condition of gameplay causes significant concerns about the quality of considerations about user privacy and security. Given the game's popularity and rich data collection capabilities, it is sure to be a prime target for hackers and bad performers. Niantic must take precautions to protect the security of user information and to communicate the methods by which you are securing sensitive information.

  As such, we urge you to:

  - Only collect the personal data necessary to provide users with the Pokémon GO gameplay experience.
  - Retain data only for as long as is necessary to serve a business purpose clearly defined and articulated in your Privacy Policy, and restricted to the uses to which parents or users have consented. This extends to deleting location data collected about users that is no longer needed to play the game, and not sharing location data about players under 13 with advertisers.
  - Establish strong safeguards to protect data from unauthorized access, including blocking access to other users, protecting data transmitted while using the app, and limiting access to any data that is retained.

- **Don't treat children as a "business asset:"** Given the popularity of the game and its appeal to children, there exists an unprecedented opportunity to accumulate broad swaths of personal data on millions of children. In his July 12 letter to Niantic, Senator Al Franken posed the idea that many children will play Pokémon GO whose data is considered a "business asset" under Niantic's Privacy Policy. We fundamentally object to the notion that the sensitive personal information of children should be considered a business asset. Rather, significant care must be taken to protect this information from improper use or access. This information, particularly children and teen's location data, should not be used to develop profiles of kids that are bought and sold. As Niantic seeks to capitalize on every potential revenue stream associated with Pokémon GO, we

urge you to adopt the policy that sensitive personal information of children is not, and should not be, for sale.

In summary, on behalf of the millions of parents and children playing Pokémon GO, we ask that Niantic:

1) **Obtain informed and meaningful consent from parents,** including by providing a clearer delineation between in-app purchases that require cash, and items that can be purchased using game currency, and make it easy for parents to understand how much money their children have spent;
2) **Take specific precautions to protect children's physical safety,** and explain how you proactively work to protect the safety of children and teen players;
3) **Ensure privacy and security from the ground up,** including putting in place a data sunset on storing location data collected from children and teens; and
4) **Don't treat children as a "business asset,"** including by committing to not use location data to build profiles and target ads to children and teens.

I would like to set up a meeting in the coming weeks to discuss the concerns raised in our letter and I look forward to your response to the suggestions we are making to ensure greater privacy, security, and safety of the millions of children playing Pokemon GO.

Sincerely,

James P. Steyer
Founder and CEO
Common Sense

CC:

The Honorable Members of the U.S. Senate Committee on Commerce
The Honorable Members of the U.S. House Committee Energy & Commerce
The Honorable Senator Al Franken
The Honorable Senator Elizabeth Warren
The Honorable Senator Mark Warner