



July 22, 2016

Chairwoman Edith Ramirez
The Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Dear Chairwoman Ramirez and FTC Commissioners:

We are writing to you regarding the data collection practices of Niantic, Inc. (“Niantic”), a former Google company and the developer of the Pokemon GO app. As you are likely aware, Niantic granted itself full access to users’ Google accounts when it first released the Pokemon GO app. This was almost certainly in violation of the Federal Trade Commission’s (“FTC”) earlier consumer privacy decisions and posed an enormous security risk to millions of Internet users who downloaded the app.¹ The company concedes that it made a serious mistake, but questions remain about the scope of Niantic’s ongoing data collection practices, a similar episode involving Google Street View and the Niantic CEO, as well as Niantic’s ongoing relationship with Google. These questions raise important privacy issues that we urge the Federal Trade Commission (“FTC”) to pursue.

The Developers of Pokemon GO Have Repeatedly Disregarded Consumer Privacy and Security

When Niantic released Pokemon GO, the company granted itself “full access” to the accounts of users who signed up for the game with a Google account.² Full account access allowed the company to view users’ contacts; view and send e-mail; view and delete Google Drive documents; access search and map navigation history; and view private photos stored in Google Photos.³ At no time did Niantic request user permission for full access to Google accounts; users simply logged in to the app via their Google account without receiving any

¹ Adam Reeve, *Pokemon Go is a Huge Security Risk*, TUMBLR (July 8, 2016), <http://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk>.

² Adam Reeve, *Pokemon Go is a Huge Security Risk*, TUMBLR (July 8, 2016), <http://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk>.

³ Andrew Cunningham, *iOs Version of Pokemon Go is a Possible Trainwreck*, Ars Technica (July 11, 2016), <http://arstechnica.com/gaming/2016/07/pokemon-go-on-ios-gets-full-access-to-your-google-account/>; Adam Reeve, *Pokemon Go is a Huge Security Risk*, TUMBLR (July 8, 2016), <http://adamreeve.tumblr.com/post/147120922009/pokemon-go-is-a-huge-security-risk>. *But see* Violet Blue, *Don’t Believe the ‘Pokemon Go’ Privacy Hype*, ENGADGET (July 15, 2016), <https://www.engadget.com/2016/07/15/dont-believe-the-pokemon-go-privacy-hype/>.

additional information about what data will be accessed.⁴ During this time, all users' full accounts were at risk of hacking and data breach. The FTC has previously found similar practices to be unfair or deceptive.⁵

After widespread public attention⁶ to this invasive overreach, Niantic and Google responded by reducing Niantic permissions to access users' basic Google account profile information.⁷ Now, when users sign into the app through their Google account –the only option currently available – Niantic can view users' email addresses and associate users with their public Google profiles.⁸

Notably, this is not the first time that Niantic's founder and CEO, John Hanke, has been at the center of a privacy controversy. Hanke was a co-founder of Keyhole, the company purchased by Google to develop Google Earth.⁹ While at Google, Hanke oversaw the development of Google Maps, Earth, and Street View.¹⁰ Google Street View raised serious privacy concerns when it launched in 2007, sparked by the collection and display of images obtained by the Google Street View cameras.¹¹ Google initially defended the program from privacy objections with promises that they "have been careful to only collect images that anyone could see walking down a public street" and would "be sure to respect local laws."¹²

However, in May 2010, following an investigation by an independent privacy agency in Germany, Google admitted it had collected a vast amount of Wi-Fi data.¹³ As the New York Times explained at the time, "European privacy regulators and advocates reacted angrily Saturday to the disclosure by Google, the world's largest search engine, that it had systematically collected private data since 2006 while compiling its Street View photo archive."¹⁴ As the

⁴ *Id.*

⁵ See, e.g., *Compete, Inc.*, 155 F.T.C. 264 (2013).

⁶ Natasha Lomas, *Pokemon Go Wants to Catch (Almost) All Your App Permissions*, TechCrunch (Jul. 11, 2016), <https://techcrunch.com/2016/07/11/pokemon-go-wants-to-catch-almost-all-your-permissions/>; Devin Coldewey, *Pokemon Go Shouldn't Have Full Access to Your Gmail, Docs, and Google Account — But it Does*, TechCrunch (Jul. 11, 2016), <https://techcrunch.com/2016/07/11/pokemon-go-shouldnt-have-full-access-to-your-gmail-docs-and-google-account-but-it-does/>; @JJAbraham, Twitter, <https://twitter.com/jjabraham/status/752612229065936896>; @Jose_Pagliery, https://twitter.com/Jose_Pagliery/status/752684763023040513.

⁷ Sarah Perez, *Pokemon Go Promises to Fix the Bug That Let It Access All of Your Google Data*, TechCrunch (July 12, 2016), <https://techcrunch.com/2016/07/12/pokemon-go-promises-to-fix-the-bug-that-let-it-access-all-your-google-data/>

⁸ Apps Connected to Your Account, Google <https://support.google.com/accounts/answer/3466521?hl=en>.

⁹ Glixel Staff, *Why We Won't See More Games Like 'Pokemon Go,'* ROLLING STONE (July 19, 2016), <http://www.rollingstone.com/culture/news/why-we-wont-see-more-games-like-pokemon-go-w429840>.

¹⁰ *Id.*

¹¹ See EPIC, *Investigations of Google Street View*, <https://epic.org/privacy/streetview/>

¹² Peter Fleischer, *Street View and Privacy*, Google Maps (Sep. 24, 2007), <https://maps.googleblog.com/2007/09/street-view-and-privacy.html>.

¹³ Alan Eustace, *WiFi Data Collection: An Update*, Google Blog (June 9, 2010), <https://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>.

¹⁴ Kevin O'Brien, *Google Data Admission Angers European Officials*, N.Y. TIMES (May 15, 2010), <http://www.nytimes.com/2010/05/16/technology/16google.html>.

investigation unfolded, it became clear that Google sought to conceal the scope of data collection that had occurred.¹⁵

Google had originally admitted to collecting fragments of Wi-Fi data, but was forced to concede that it had collected more than just fragments. Google revealed that it gathered MAC addresses (the unique device ID for Wi-Fi hotspots) and network SSIDs (the user-assigned network ID name) tied to location information for private wireless networks. Google also admitted that it intercepted and stored Wi-Fi transmission data, stating that “in some instances entire emails and URLs were captured, as well as passwords.”¹⁶

An investigation by the Federal Communications Commission revealed “the data collection resulted from a deliberate software-design decision by one of the Google employees working on the Street View project.”¹⁷ The engineer responsible for this design decision was Marius Milner. Notably, both Milner and Hanke are listed as co-inventors in a patent for a “location-based parallel reality game” assigned to Google, Inc. Hanke’s Niantic Labs began as an internal start-up at Google, where it developed the augmented-reality game Ingress that laid the foundation for Pokemon GO.¹⁸ Niantic was later spun out of Google in 2015.¹⁹

History suggests Niantic will continue to disregard consumer privacy and security, which increases the need for close FTC scrutiny as Niantic’s popularity – and trove of sensitive user data – continues to grow. Moreover, given the prior history of Google Street View, there is little reason to trust the assurance regarding the current state of Niantic’s data collection practices.

Niantic’s Extensive Data Collection Exceeds Functionality Needs for the Pokemon GO App

According to the Pokemon GO Privacy Policy, Niantic collects a vast amount of data including users’ email addresses; user names; messages sent to other users; device identifiers; user settings; device operating systems; Internet Protocol (IP) addresses; and the web page last visited before accessing the app.²⁰ When users sign in to the app through their Google account – the only option currently available – Niantic can view users’ email addresses and associate users with their public Google profiles.²¹ Niantic does not explain the scope of information gathered from Google profiles or why this is necessary to the function of the Pokemon GO app.

¹⁵ Kevin J. O’Brien, *Europe Pushes Google to Turn Over Wi-Fi Data*, N.Y. TIMES (June 27, 2010), <http://www.nytimes.com/2010/06/28/technology/28google.html>.

¹⁶ Alan Eustace, *Creating Stronger Privacy Controls Inside Google*, Google Blog (Oct. 22, 2010), <https://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html>.

¹⁷ Google Inc., Notice of Apparent Liability for Forfeiture, DA 12-592.

¹⁸ Robinson Meyer, *The Curious Mystery of the Map in Pokemon Go*, THE ATLANTIC (July 11, 2016), <http://www.theatlantic.com/technology/archive/2016/07/where-did-pokemon-go-get-its-map/490799/>.

¹⁹ *Id.*

²⁰ Pokemon GO Privacy Policy, Niantic (July 1, 2016), <https://www.nianticlabs.com/privacy/pokemongo/en> [hereinafter “Niantic Privacy Policy”].

²¹ Apps Connected to Your Account, Google <https://support.google.com/accounts/answer/3466521?hl=en>.

Niantic also collects users' precise location information through "cell/mobile tower triangulation, wifi triangulation, and/or GPS."²² Although users have the ability to limit location collection to when the app is in use, many keep the app open at all times to receive alerts of potential game activity nearby. The Privacy Policy states Niantic will "store" location information and "some of that location information, along with your ... user name, may be shared through the App."²³ The Privacy Policy does not indicate any limitations on how long Niantic will retain location data, how it will use this data, or with whom it will be shared. Nor does Niantic explain how indefinite retention of location data is necessary to the functionality of the Pokemon GO app. As one industry expert warned, "Pokémon Go's incredibly granular, block-by-block map data, combined with its surging popularity, may soon make it one of, if not *the most*, detailed location-based social graphs ever compiled."²⁴ Experts predict that much of the geolocation data app-makers receive "probably isn't truly being monetized and utilized to its fullest potential" and with the data's high latent value, the "ultimate goal is a buyout."²⁵

With Pokemon GO, Niantic has access to users' mobile device camera.²⁶ The Terms of Service for Pokemon GO grant Niantic a "nonexclusive, perpetual, irrevocable, transferable, sublicensable, worldwide, royalty-free license" to "User Content."²⁷ The Terms do not define "User Content" or specify whether this includes photos taken through the in-app camera function. As one privacy expert warned, "What's noticeably absent, however, is any mention of what the company does with information collected by the device camera."²⁸

The Pokemon GO Privacy Policy grants Niantic wide latitude to disclose user data to "third-party service providers," "third parties," and "to government or law enforcement officials or private parties as [Niantic], in [its] sole discretion, believe necessary or appropriate."²⁹ Niantic also deems user data, including personally identifiable information, to be a "business asset" that it can transfer to a third party in the event the company is sold.³⁰ The Policy also states that user data may be transferred to international locations "where the privacy laws may not be as protective as those in [users'] jurisdiction."³¹ As one expert observed, in light of Niantic's broad

²² Niantic Privacy Policy.

²³ *Id.*

²⁴ Joseph Bernstein, *You Should Probably Check Your Pokemon Go Privacy Settings*, BUZZFEED NEWS (July 12, 2016), https://www.buzzfeed.com/josephbernstein/heres-all-the-data-pokemon-go-is-collecting-from-your-phone?utm_term=.gf0qBd39l#.mnJpRaq5W.

²⁵ John Divine, *Pokemon Go: Collecting All the Data?*, U.S. News & World Report (July 13, 2016), <http://money.usnews.com/investing/articles/2016-07-13/pokemon-go-collecting-all-the-data>.

²⁶ Pokemon GO, Google Play (July 20, 2016),

<https://play.google.com/store/apps/details?id=com.nianticlabs.pokemongo&hl=en>.

²⁷ Pokemon GO Terms of Service, Niantic (July 1, 2016),

<https://www.nianticlabs.com/terms/pokemongo/en> [hereinafter "Pokemon GO TOS"].

²⁸ Jedidiah Bracy, *Pokemon GO, Augmented Reality, and Privacy*, IAPP (July 11, 2016),

<https://iapp.org/news/a/pokemon-go-augmented-reality-and-privacy/>.

²⁹ Niantic Privacy Policy.

³⁰ *Id.*

³¹ *Id.*

statements regarding disclosure of user data and its close ties to Google, “it’s prudent to expect some of your location data to end up in Google’s hands.”³²

In addition, Niantic retains “information (including your....profile information) and user content for a commercially reasonable time period....following termination or deactivation of a user’s account” and “some information...in archived/backup copies for our records or as otherwise required by law.”³³ Also under the Terms of Service, users are forced into binding arbitration unless they opt-out within 30 days of first accessing the app.³⁴

U.S. Senator Al Franken recently voiced concern over the extent to which Niantic may be unnecessarily collecting, using, and sharing a wide range of users’ personal information.³⁵ He called on Niantic to identify which features of the game require information collection and access to mobile capabilities, whether the data collection is used for other purposes, and if Niantic would consider making data collection that is unnecessary to the operation of the game an opt-in feature as opposed to opt-out. Pokemon Go shares de-identified and aggregate data with other third parties, but does not meaningfully describe the purposes for which it shares or sells the data. Consumers are unable to reasonably avoid potential harm from third party disclosures and are not informed of the ways in which the data may be used by third parties.³⁶

Niantic’s Data Policies Fail to Comply with Fair Information Practices and Constitute Unfair Business Practices

Public attention to the privacy implications of Niantic’s Pokemon GO app have focused primarily on Niantic’s failure to disclose its full access to users’ Google accounts. This focus is misguided, and does not consider the significant privacy and security risks the app continues to pose to its millions of users worldwide. Reliance on disclosure or “notice and choice” places the burden on consumers to navigate increasingly complex privacy policies³⁷ and provides no substantive privacy protections.³⁸

The FTC must instead use its unfairness authority under Section 5 of the Federal Trade

³² Natasha Lomas, *Pokemon GO Wants to Catch (Almost) All Your App Permissions*, TECHCRUNCH (July 11, 2016), <https://techcrunch.com/2016/07/11/pokemon-go-wants-to-catch-almost-all-your-permissions/>.

³³ Niantic’s “clients, affiliates, or service providers” may also retain this information.

³⁴ Pokemon GO TOS.

³⁵ Letter from Al Franken, U.S. Senator, to John Hanke, CEO of Niantic (July 12, 2016), http://www.franken.senate.gov/files/letter/160712_PokemonGO.pdf.

³⁶ Letter from Al Franken, U.S. Senator, to John Hanke, CEO of Niantic (July 12, 2016), http://www.franken.senate.gov/files/letter/160712_PokemonGO.pdf.

³⁷ See Rick Noack, *How Long Would It Take to Read the Terms of Your Smartphone Apps? These Norwegians Tried It Out*, WASH. POST (May 28, 2016)

<https://www.washingtonpost.com/news/worldviews/wp/2016/05/28/how-long-would-it-take-to-read-the-terms-of-your-smartphone-apps-these-norwegians-tried-it-out/> (reporting an experiment where it took more than 31 hours to read the terms and conditions of 33 popular apps).

³⁸ See EPIC Reply Comments to FCC, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (July 6, 2016), <https://www.epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf>.

Commission Act³⁹ to prohibit practices by Niantic and other augmented-reality apps that fail to conform with Fair Information Practices (“FIPs”). President Obama’s 2012 formulation of FIPs in the Consumer Privacy Bill of Rights (“CPBR”) offers a comprehensive framework to protect against unfair and deceptive practices.⁴⁰ The CPBR espouses the following practices: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, and Accountability.⁴¹

Niantic’s failure to comply with FIPs, particularly with its unlimited collection and indefinite retention of detailed location data, is “likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”⁴²

Collecting and compiling detailed maps of consumers’ location history causes substantial injury to consumers by posing serious safety and privacy risks of abusive data practices and identity theft.⁴³ Mobile apps have increasingly become the target of hackers because of the sheer volume and sensitivity of valuable data they collect.⁴⁴ Unsurprisingly, Pokemon has already been the target of a cyberattack⁴⁵ and has received threats of future, more damaging hacks.⁴⁶

These risks cannot be reasonably avoided because users must completely delete the Pokemon GO app and quit playing this popular game to stop Niantic from tracking their location. Consumers are thus forced to choose between forgoing their privacy interests and forgoing Pokemon GO, and there is no means for users to play the game while preventing their location information from being collected and retained indefinitely. There is no evidence that Niantic’s collection and retention of location data is necessary to the function of the game or otherwise provides a benefit to consumers that outweighs the privacy and safety harms it creates.

³⁹ 15 U.S.C. § 45.

⁴⁰ See EPIC, *White House: Consumer Privacy Bill of Rights*, https://epic.org/privacy/white_house_consumer_privacy_.html.

⁴¹ *Id.*

⁴² 15 U.S.C. § 45(n).

⁴³ See *Complaint, Request for Investigation, Injunction, and Other Relief Submitted by The Electronic Privacy Information Center in the Matter of Uber Technologies, Inc.* (June 22, 2015), <https://epic.org/privacy/internet/ftc/uber/Complaint.pdf> (discussing Uber’s regular abuse of its access to customers’ locations).

⁴⁴ See, e.g., Alexandra McDonald, Jason McDonell, Caroline Mitchell, *Mobile Apps: Redefining the Virtual California Economy and the Laws That Govern It*, 24 Competition: J. Anti. & Unfair Comp. L. Sec. St. B. Cal. 86, 102 (2015); *Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration*, Gartner (May 29, 2014), <http://www.gartner.com/newsroom/id/2753017>; Dan Goodin, *1,500 iOS apps have HTTPS-crippling bug. Is one of them on your device?*, Ars Technica (April 20, 2015), <http://arstechnica.com/security/2015/04/1500-ios-apps-have-https-crippling-bug-is-one-of-them-on-your-device/>; <https://sourcedna.com/blog/20150420/afnetworking-vulnerability.html>.

⁴⁵ Carli Velocci, *Pokémon Go Servers Reportedly Attacked Because It Was Bound to Happen*, Gizmodo (July 16, 2016), <http://gizmodo.com/pokemon-go-servers-reportedly-hacked-because-it-was-bou-1783779474>.

⁴⁶ Melanie Ehrenkranz, *Hackers Just Issued a Huge Threat to Every ‘Pokemon Go’ Player*, Time (July 20, 2016), <http://time.com/4415034/pokemon-go-hackers-poodlecorp/>.

Niantic's Unlimited Collection and Retention of User Data Violates COPPA

Niantic's unlimited collection and indefinite retention of detailed location data violate the data minimization requirements under the Children's Online Privacy Protection Act (COPPA), which requires providers to "retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected."⁴⁷ Niantic does not disclose how long location information is retained or what purpose this retention fulfills.

The FTC Must Investigate Niantic's Unfair and Deceptive Practices and COPPA Violation

The Pokemon GO app raises complex and novel privacy issues that require close FTC scrutiny. Niantic's disappointing history with respect to consumer privacy further underscores the need for FTC oversight. The FTC should (1) investigate whether Niantic's data collection and retention practices are consistent with FIPs; (2) prohibit Niantic's policies that are inconsistent with FIPs as unfair or deceptive trade practices; and (3) investigate Niantic's ongoing COPPA violations.

Thank you for your consideration of this request. We look forward to working with you on these important issues.

Respectfully Submitted,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President and Executive Director

/s/ Claire Gartland

Claire Gartland
EPIC Consumer Protection Counsel

/s/ Natashí Amlani

Natasha Amlani
EPIC IPIOP Clerk

Cc: U.S. Senator Jeff Flake
U.S. Senator Al Franken
U.S. Representative Fred Upton
U.S. Representative Frank Pallone

⁴⁷ 16 C.F.R. § 312.10.