

August 10, 2022

Purnima Kochikar
VP of Google Play
kochikar@google.com

Lee Milstein
Head of SDK Partnerships
lmilstein@google.com

Re: Query_All_Packages Permission – Necessity of Permission for Online Gaming Apps

Dear Ms. Kochikar and Mr. Milstein:

Our association, the iDevelopment and Economic Association (“iDEA”) submits this letter regarding online interactive businesses’ critical need for the Query_All_Packages Permission (“QAP Permission”) in the Google Play store. The QAP Permission gives visibility into the inventory of installed apps on a given device to be used for security and compliance purposes.

As background, iDEA is a non-profit association of gaming industry stakeholders who seek to grow jobs and expand lawful online interactive business in the United States through advocacy and education. iDEA represents the legislative and regulatory interests of national and international businesses – including our 30+ [members](#) – with online interactive entertainment platforms that are operating, or that are considering operating, in U.S. states that have legalized interactive gaming. Among other things, the association aims to (i) educate lawmakers, enforcement agencies and the general public; (ii) develop industry best practices and standards around responsible gaming; and (iii) support positive legislation that broadens the U.S. market for safe and successful regulated online gaming.

iDEA Members Require Query_All_Packages to Ensure Compliance with Federal and State Laws

We understand that the Google Play store has announced a policy update that would restrict updates to applications (or “apps”) or submission of new apps utilizing the QAP Permission unless a declaration is filed with Google and Google approves the request. In turn, to qualify for the QAP Permission, the app must fall within certain “permitted uses” and “have a core purpose to search for all apps on the device.” In addition, Google requires the app “justify why a less intrusive method of app visibility will not sufficiently enable your app’s policy-compliant user-facing core functionality.” (Core functionality being “the main purpose of the app”).

“Permitted uses involve apps that must discover any and all installed apps on the device, for awareness or interoperability purposes may have eligibility for the permission. Permitted uses include device search, antivirus apps, file managers, and browsers.”¹

Google Play provides an exception to its policy for certain applications, namely “Apps that have a verifiable core purpose involving financial-transaction functionality (for example, dedicated banking and dedicated digital wallets) may obtain broad visibility into installed apps solely for security-based purposes.”²

Our members believe that their need for the QAP Permission should be permitted under Google’s existing policies. As described below, online gaming apps have a “verifiable core purpose involving financial-transactional functionality” and need broad visibility into installed apps “solely for security-based purposes.” In particular, online gaming apps are required by state and federal law to verify a user’s location when the user accesses his or her account and to apply dynamic checks based on a user’s proximity to the border while identifying and blocking methods to circumvent these controls. This geolocation requirement is to ensure that a user’s wagering transaction occurs solely within the borders of the applicable state, as mandated by federal and state law or regulation. The apps need QAP Permission to scan for any apps that could be used to spoof a user’s geolocation. This is critical to the security and operation of the online gaming app, as required by applicable laws.

However, our members have recently become aware that Google’s policy may be interpreted to prevent online gaming applications from providing updates and barring their use of the QAP Permission. We appreciate that Google has worked with industry to better understand our concerns and has allowed gaming applications additional time beyond the previously announced deadline, while Google reviews its policy and the industry’s need for the QAP Permission. On behalf of the industry, we provide additional background to assist Google in its analysis.

Online Gaming Operates in a Heavily Regulated Environment that Requires Geolocation and QAP Permission

The online gaming industry has flourished during the past several years, following court decisions and legislative activity to permit online gaming activities. For example, over 30 states currently permit sports betting within their borders, and the industry is heavily regulated. State

¹ <https://support.google.com/googleplay/android-developer/answer/10158779#zippy=%2Cexceptions%2Cinvalid-uses%2Cpermitted-uses-of-the-query-all-packages-permission>.

² *Id.*

regulators carefully vet potential licensees. Once licensed, operators are subject to extensive regulatory mandates governing such obligations as anti-money laundering, integrity, data security, and patron identity verification. A critical component of online gaming in every state is that participants must be located within the borders of the state. This requirement stems from certain federal laws, including the Unlawful Internet Gambling Enforcement Act (“UIGEA”) and the Wire Act, which exempt online gaming from federal restrictions on gambling, provided the activities are authorized by state law and are conducted on an *intrastate* (rather than interstate) basis.

For example, UIGEA makes it a federal crime for a knowing receipt by a person “in the business of betting or wagering” of monies in connection with the participation of another person in “unlawful Internet gambling.”³

The UIGEA term “unlawful Internet gambling” exempts online gambling activity where the following conditions are met:

*“(i) the bet or wager is initiated and received or otherwise made exclusively **within a single State**;*

(ii) the bet or wager and the method by which the bet or wager is initiated and received or otherwise made is expressly authorized by and placed in accordance with the laws of such State, and the State law or regulations include—

*(I) **age and location verification requirements reasonably designed to block access to minors and persons located out of such State**; and*

*(II) **appropriate data security standards to prevent unauthorized access by any person whose age and current location has not been verified in accordance with such State's law or regulations**; and*

(iii) the bet or wager does not violate any provision of” certain other federal laws.

To explain these requirements in practical terms, online gaming apps must ensure that someone attempting to place a wager on a Virginia online sports betting app (Virginia authorized online sports betting in 2020) is in fact in the Commonwealth of Virginia, and not in any other state (even a neighboring state of Maryland or the District of Columbia).

Listed below are specific examples of state geolocation requirements. All of the states which permit online sports betting and online casino mandate similar requirements.

³ 31 U.S.C.A. § 5363 (emphasis added).

The most common requirements for geolocation are contained within the adopted technical standard for online sports betting and online casino published by Gaming Laboratories International (GLI-33 and GLI-19 respectively). Each contain the following requirement:

2.7.2 Location Fraud Prevention

The Event Wagering System shall incorporate a mechanism to detect the use of remote desktop software, rootkits, virtualization, and/or any other programs identified as having the ability to circumvent location detection. This shall follow best practice security measures to:

- a) ***Detect and block location data fraud (e.g., fake location apps, virtual machines, remote desktop programs, etc.) prior to completing each wager;***
- b) *Examine the IP address upon each Remote Wagering Device connection to a network to ensure a known Virtual Private Network (VPN) or proxy service is not in use;*
- c) ***Detect and block devices which indicate system-level tampering (e.g., rooting, jailbreaking, etc.);***
- d) *Stop "Man-In-The-Middle" attacks or similar hacking techniques and prevent code manipulation;*
- e) ***Utilize detection and blocking mechanisms verifiable to an application level;***
and
- f) *Monitor and prevent wagers placed by a single player account from geographically inconsistent locations (e.g., wager placement locations were identified that would be impossible to travel between in the time reported).*

Every regulated market has a unique but different set of regulations, however below are two online sports betting examples:

New York:

Geolocation requirement.

*Geolocation software used by mobile sports wagering licensees **shall be approved by a licensed independent testing laboratory, including applicable field testing, before the software is deployed in this State.** Internal controls for geolocation requirements shall address:*

- (1) *how the licensee shall ensure that authorized sports bettors shall be physically located within the State of New York when engaging in mobile sports wagering;*

(2) which geolocation system will be used to reasonably detect the physical location of an authorized sports bettor attempting to place a sports wager with the skin and block unauthorized attempts to access the licensee’s platform throughout the duration of the wagering session;

(3) how the geolocation system will detect any mechanisms a bettor may use to circumvent the requirement that the bettor be physically located within the State of New York;

*(4) how the geolocation system ensures the integrity of the bettor’s account and the bettor’s device by **blocking sports wagers from devices that indicate tampering** (emphasis added).*

Colorado:

3. LOCATION DATA INTEGRITY

To ensure the integrity of location data, the Geo-location System shall:

- a. **Detect and block location data fraud (e.g. Proxy, Fake Location Apps, Virtual Machines, Remote Desktop Programs, etc.);***
- b. Utilize detection and **blocking mechanisms verifiable to a source code level;***
- c. Follow best practice security measures to stop "man in the middle" attacks and **prevent geolocation code manipulation** such as replay attacks.*

The QAP Permission is Critical to Gaming Applications by Ensuring Users or Third Parties are not “Spoofing” their Locations, which includes Preventing Hacking by Foreign and Other Actors

The industry has established that users and bad actors can attempt to “spoof” their locations in order to circumvent the geolocation requirements. For instance, a user located in a state that does not permit sports betting (e.g., Texas) may attempt to manipulate the Android operating system to make it appear he is betting from inside an authorized state (e.g., utilizing a licensed operator’s Pennsylvania sports betting application). iDEA member GeoComply, the market leader in geolocation security, has identified several thousand applications and methods which circumvent geolocation data/controls.

Below are just a few examples of methods used by users and bad actors to bypass location restrictions:

- Fake Location Apps
 - FakeGPS applications can easily can bypass location data in various ways
- Root and Root Cloaking Apps
 - Detecting rooted devices is required by gaming regulations
 - Rooted devices can manipulate location data as well as other behaviors of our app.
- Package Name Randomization
 - Randomized package names are used to evade compliance detection.
- Emulators
 - Many emulators/ device farms can be used to spoof location/control devices remotely.
 - Package names detection is important to detect all emulators/device farms
- Cloned App/Dual Space Apps
 - Cloned apps/Dual Spaces are used to hide the installed packages from us.
 - GeoComply detects them using the package names as well as an unnatural number of packages installed.

This list is illustrative – threats emerge in real-time with new methods and apps constantly changing. Geolocation cybersecurity experts need access to the QAP Permission function to detect and react to emerging threats in real-time. The QAP Permission enables state authorized geolocation verification companies (and in turn, the operators who contract with them to provide these services) to ensure that these apps and features are not being used to manipulate an individual’s accurate geolocation. Otherwise, operators will be placed in jeopardy of being noncompliant with state and federal geolocation requirements.

Gaming Operators Obtain Consent for Access to QAP Permission from Users

In establishing player accounts, state regulations mandate that operators collect and maintain accurate and complete user information with detailed information, including full name, age, residence, and an identifier such as a social security number. This is required to confirm several categories of required information. In addition to collecting this information at the point of account creation, states also require that operators verify location through the gaming session and prior to the placement of wagers. State regulations generally mandate that operators disclose this collection of information to users.

Online gaming operators disclose to users these information collection categories. Users must consent to location sharing in order to access a gaming system and this standard in practice across the industry.

Gaming Operators are Similar to Financial Institutions for QAP Permission Exception and under Privacy Laws

As discussed above, Google allows an exception for certain financial transactions requiring access to the QAP Permission. Specifically, Google allows the following apps to use the QAP Permission: “Apps that have a verifiable core purpose involving financial-transaction functionality (for example, dedicated banking, dedicated digital wallet) may obtain broad visibility into installed apps solely for security-based purposes.”

Online gaming operators utilize the QAP Permission for the core purpose of the financial transaction functionality of the gaming and fantasy sports apps. They use the QAP Permission solely to comply with federal and state requirements to confirm location status and for security-based purposes. This ensures that individuals are not using methods to circumvent these required security controls. There is no use of the QAP Permission in marketing, or in any sharing outside of the relationship between a geolocation vendor and its gaming operator customer.

As new data privacy laws and regulations continue to be introduced across the US, at both the state and federal levels, there is one constant across all proposed and enacted laws: there are clearly defined and well-established exemptions for the collection, utilization and analysis of certain forms of data, including advanced location data and intelligence, for purposes of complying with:

- An existing state or federal law (such as UIGEA, Wire Act, Bank Secrecy Act) or
- For the prevention and detection of fraud.

This standard has been consistently applied across data privacy laws that have been enacted in California, Colorado, Virginia, and Illinois, in addition to recent federal data privacy proposals, including the American Data Privacy and Protection Act.

Accordingly, the insights from the QAP permissions for purposes of 1) compliance with applicable state and federal laws (such as UIGEA; Wire Act and the Bank Secrecy Act) and 2) fraud prevention and detection, present no legal reason or precedent to restrict or limit their QAP permissions on the basis of data privacy requirements.

Lastly, the QAP permission which enables geolocation cybersecurity defense, ultimately protects users directly in the following areas:

1. Detection and prevention of account takeover/hijacking from bad actors from around the world who have obtained stolen credentials;
2. Prevention of bonus abuse and other fraud affecting the product pricing and benefits of an otherwise safe market;
3. Prevent of collusion in online peer-to-peer games where a user can occupy multiple positions and spoof location to avoid detection;
4. Prevent underage or other unauthorized users from accessing gambling systems from countries/states where it is illegal to do so; and
5. Preventing users from committing federal and/or state crimes by knowingly or unknowingly accessing gambling systems via widely available geolocation spoofing tools installed on their devices which may be available from the Play Store.

Impacts on the Gaming Industry Will be Dire

If Sports betting and other online gaming operators cannot access the QAP Permission, they will not be able to prove compliance with federal and state law and therefore will not be able to deploy Android applications. Users who want to engage in sports betting will have to find other sources.

Ultimately, the removal of the permission may create dire consequences, including:

1. Creating an environment where operators are not able to effectively block targeted fraud, protect users and operators from non-compliant activity, and prevent financial transactions from sanctioned countries such as Russia and Iran
2. Creating an environment where regulators are forced to restrict the availability of gambling applications from the Play Store.
3. Impacting Google performance marketing, as online gaming operators will not be using Google services to promote offerings.

Conclusion

iDEA and its member companies look forward to working with Google to provide any further information that would be helpful to Google to understand the critical need for the QAP Permission for our industry. We would be pleased to set up an in-person or virtual meeting to discuss these issues, or to provide additional details from our member companies.

We understand that state regulators will also be contacting Google Play to detail their concerns. Thank you for your attention to this matter.

Sincerely,



Jeff Ifrah
General Counsel, iDEA
jeff@ifrahlaw.com
(202) 524-4142

iDEA Members

- 888
- Bet365
- Catena Media
- Continent 8
- Digital Gaming Corp
- DraftKings
- EML Payments
- Entain
- EveryMatrix
- Evolution Gaming
- FanDuel
- Fox Bet
- Gamesys
- GeoComply
- Global Payments
- Golden Nugget
- Ifrah Law
- Kambi
- Kindred
- Pala Interactive
- Paysafe
- Playtech
- Pointsbet
- Resorts Digital Gaming
- Saiber Law
- Scientific Games
- Shift4
- Sightline
- Sportradar
- White Hat Gaming
- Worldpay