March. 22, 2013

Charles A. Harwood, Acting Director
Bureau of Consumer Protection
United States Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Formal Complaint Regarding Google's Second Violation of Buzz Order

Dear Mr. Harwood,

On February 25, I wrote you on behalf of Consumer Watchdog requesting immediate Commission action to address Google's most recent violation of the Buzz Consent Order (and Google's own privacy policy) – the disclosure of confidential user information to independent application developers. Thank you for referring my original letter to the Enforcement Division; we trust a serious investigation of Google's egregious actions is underway. I am writing now to bring to your attention additional information that has recently come to light.

First Consumer Watchdog Letter

In my earlier letter, I explained that most Google services require users to provide Google with personal information, including users' names, email addresses, telephone numbers, and credit card numbers, all of which the company promises to keep confidential in its general Privacy Policy. The specific privacy policy for Google Wallet (the Google service through which users buy device applications) permits the sharing of confidential information outside the company in only three narrow circumstances:

> We will only share your personal information with other companies or individuals outside of Google in the following circumstances:
> - As permitted under the Google Privacy Policy,
> - As necessary to process your transaction and maintain your account,
> - To complete your registration for a service provided by a third party.

According to numerous press reports cited in my February 25 letter, Google regularly distributes confidential user information to application developers. By disclosing personal information in this manner, as my letter details, Google enables the association of individual users with sensitive private subjects, including health conditions, sexual activity, sexual orientation, and online dating. Google's conduct violates Section 5 of the FTC Act, the company's own privacy policy, and the Buzz Consent Order – which (at Part III) prohibits Google from misrepresenting "the extent to which [it] maintains and protects the privacy and confidentiality" of, among other things, users' names, email addresses and physical locations.

Google's Response to Congressman Johnson

Last week, Google made a formal written response to a set of questions from Congressman Hank Johnson regarding its disclosure of confidential user information to application developers. (Google response attached.) As I predicted in my earlier letter, Google attempted to defend its conduct by pointing to the "as necessary to process your transaction and maintain your account" language in the Google Wallet privacy policy. Rather than justifying its conduct, Google's argument demonstrated that the company lacks any satisfactory explanation for its practices.

In its response to Congressman Johnson, Google did not challenge the accuracy of widespread reports that the company routinely discloses confidential information to applicant developers regarding all users who purchase applications from Google. For purposes of evaluating Google's conduct under the Buzz Consent Order, then, it can be taken as fact that Google engages in this behavior.

Certainly, Google implied in its response that users know or should have assumed that the company would share confidential user identification information with application developers. But that suggestion directly contradicts the privacy representations made by Google to users – that users should feel secure because Google will not willy nilly share their information – but will only disclose confidential information when "necessary" to process the user's transaction. More specifically, Google responded to Congressman Johnson as follows:

> Information such as name and email address is necessary for developers to issue refunds, reversals, payment adjustments – all of which developers are responsible for under the Seller Terms of Service – and investigate chargebacks.

"Refunds, reversals, payment adjustments" are not the transactions at issue in this matter. Rather, Google's privacy policy misrepresentation goes to the initial user purchase transactions for device applications. As I noted in my earlier letter, developers do not need users' private information for the initial purchase transactions. They have routinely processed such transactions without using confidential user information. Google never contests this fact in its response to the congressman.

Indeed, assuming everything Google says in its letter to Congressman Johnson is true, developers only need the users' confidential information when a request for a refund, reversal or payment adjustment is made. The disclosure exception Google points to in its policy ("necessary to process your transaction") might justify Google giving confidential information to developers for specific users who request refunds (and the like), but not for every single user who made an application purchase. So, Google violated its pledge to protect the confidentiality of millions of users who bought applications in good faith reliance on Google's public statements and who never sought a refund, reversal or payment adjustment.

In response to Congressman Johnson, Google also proffered a second justification for disclosing user information to developers:

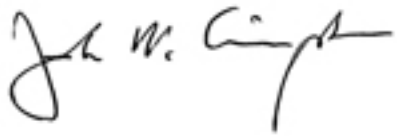
> Developers are also obligated under the Seller Terms of Service to pay applicable taxes imposed in transactions and need customer address information in order to properly calculate any local tax obligations.

This second explanation also fails to justify Google's conduct. I understand that Google pays all of the taxes on application purchase transactions and that developers merely get checks from Google for the net amounts they are owed. But even if this were not the case, a developer would need nothing more than a user's state and locality in order to pay local taxes that have been collected through the purchase process. The users' names, email addresses and phone numbers that Google discloses to application developers are not necessary in any way for the developer to calculate local tax obligations.

Renewed Request for Action

Again, thank you for referring my original letter to the Enforcement Division; we trust a serious investigation of Google's actions has been started. Google's most recent violation of the Buzz Consent Order is a matter of intense concern to Consumer Watchdog, to other privacy advocacy groups, to apps users across the country, and to the press. Although given the opportunity by Congressman Johnson, Google has yet to come up with a credible justification for its inappropriate conduct. Indeed, the letter to the Congressman in fact makes Google's violations clear. We therefore renew our request for the Commission to take strong action against Google. Thank you for your consideration.

Sincerely,



John M. Simpson
Privacy Project Director

cc: Chair Edith Ramirez, Commissioner Julie Brill, Commissioner Maureen K., Ohlhausen, Commissioner Joshua D. Wright, California Attorney General Kamala Harris and Supervising Deputy Attorney General for Privacy Enforcement and Protection Adam Miller

Attachment: Letter from Google to Rep. Hank Johnson

Tuesday, March 12, 2013

The Honorable Hank Johnson
2240 Rayburn House Office Building
Washington, DC 20515

Dear Congressman Johnson:

Thank you for your letter of February 21, 2012 about purchasing apps on Google Play. We are pleased to answer your questions and welcome the opportunity to clear up any misconceptions about Google Play developer obligations with respect to buyers' personal information.

Below we respond to your specific questions about consumers' expectations when purchasing apps on Google Play.

(l) Unlike some competitors in the mobile app ecosystem, Google acts as a marketplace for developers to exchange goods and services with consumers.

a. Please describe how an open marketplace benefits consumers.

Mobile platforms are supported by an ecosystem of apps and developers. Without such an ecosystem, users would find mobile platforms less useful because devices would be limited to pre-installed software.

To promote their ecosystems, most mobile platform providers operate a store where users can download apps for that particular platform (e.g., Apple's App Store and iTunes, Microsoft's Windows Store, Amazon Appstore, and Nokia's Ovi Store). Google developed Google Play as a store for Android apps, games and digital content, including music, movies, books and magazines.

Consistent with the philosophy behind Android, Google Play is an open and non-exclusive store where third party developers can make their Android apps available to users, either for free or at a charge. Google Play's open approach means that any developer can make apps available on Google Play (unless and until the developer's participation has been banned because of a violation of our policies, as described below), and that Google does not control or pre-approve apps before they are made available on Google Play.

An open approach in Google Play benefits consumers in many ways. For example, in an open store model, developers have a more direct engagement with their customers. This creates a feedback loop between customers and developers that we believe leads to higher product quality and customer satisfaction. Developers are able to act as small business owners, engaging with customers directly, taking their feedback, and modifying their product accordingly. Reduced barriers to publishing and updating apps also allow for

more iterative development cycles leading to higher product quality and thus greater consumer satisfaction. This also means developers are less likely to lose sales or to need to provide customer support for older versions of their apps, which can translate into lower costs to consumers and higher product satisfaction.

Google Play does automatically scan apps for potentially malicious software without disrupting the Google Play user experience or requiring developers to go through an application approval process. The service analyzes new applications, applications already in Google Play, and developer accounts. More information on this issue appears in the response to question 4(a) below.

b. How does a Consumer's experience on Google Play via a mobile device compare with their experience purchasing goods in other marketplaces?

Individuals who purchase digital goods directly from electronic merchants are typically required to provide the merchant with credit card or bank account details in addition to other personal information. For Google Play transactions, Google Wallet is the payment processor, so that consumers interact with a single trusted payment processor in that marketplace. Google Wallet does not share buyers' full payment card details with their merchants. The information apart from payment credential details that is displayed to merchants in connection with Google Play transactions is the type that buyers typically give electronic goods merchants directly for online digital commerce.

When a user purchases an application from an app developer, Google shares information as necessary to process transactions and maintain accounts. This type of information allows developers to maintain a direct relationship with their customers, meet their obligations under the Seller Terms of Service, and communicate with customers to issue refunds and payment adjustments, investigate chargebacks, and resolve other customer service issues. In many cases, app developers are able to use this information to take feedback from consumers directly to improve their product and to announce new features or fixes. However, as previously mentioned, in contrast to buyers who purchase electronic goods from merchants directly, Google Play is not sharing full payment card details with developers.

Application developers support the approach implemented by Google Play. In an article by Barry Schwartz on Marketing Land, an app developer explains: "Google, in my opinion, does it right by making the user who downloads the app our customer. We can better service them by being able to refund them, look up order status issues, and potentially contact them with issues they may have."

(2) Please discuss the types of information shared with developers through Google Wallet.

We have disclosed in the Google Wallet Privacy Notice[1] since 2006 that we may share your personal information with third parties as necessary to process your transaction and maintain your account. In that vein, depending on the type of purchase the buyer makes, we may share name, email address, address information, country, and phone number with developers.

a. How is this information necessary for developers to process transactions?

[1] Google Wallet was previously known as Google Checkout.

Information such as name and email address is necessary for developers to issue refunds, reversals, payment adjustments — all of which developers are responsible for under the Seller Terms of Service — and investigate chargebacks. Developers are also obligated under the Seller Terms of Service to pay applicable taxes imposed on transactions and need customer address information in order to properly calculate any local tax obligations.

For apps that are free to download, the Google Play purchase flow is designed to avoid sharing any of the information described above with developers because such information is not necessary to process transactions and maintain the accounts.

b. What other purposes does sharing this information serve?

We share information with developers as necessary to process transactions and maintain accounts. This type of information allows developers to maintain a direct relationship with their customers and meet their obligations under the Seller Terms of Service to issue refunds and payment adjustments and investigate chargebacks.

c. How is the breadth of information shared proportionate to Google's need to share it?

Individuals purchasing on Google Play are purchasing directly from the application developer, who is also the merchant of record. Google Wallet serves as a payment processor for the developer and thus we share information with developers as necessary to process transactions and maintain accounts. This includes making certain information accessible to merchants in order for merchants to service their customers' accounts and meet local tax obligations. As explained above, we have disclosed in the Wallet Privacy Notice since 2006 that we may share information as necessary to process transactions and maintain accounts.

d. Have any harms or breaches of trust occurred because of this sharing?

Any misuse of buyer information is a violation of our terms, and to date we are aware of only a handful of complaints about the possible misuse of personal information by developers. Google Play developers are required to agree to the Play Developer Distribution Agreement (see Section 4.3) and the Seller Terms of Service (see Section 7.1), which require developers to protect the privacy and confidentiality of buyers' personal information. Our Program Policies and Guidelines also provide strict instructions on communicating with buyers, and prohibits selling or renting buyers' information or sending marketing emails to buyers without consent. When app developers violate these terms, Google has taken administrative actions ranging from issuing warnings to suspending the developer. We believe the low number of complaints we receive regarding developer misuse of buyers' information reflects that the prohibition of such misuse in our terms and the direct relationship that developers have with their customers properly align their incentives to handle customer information appropriately.

(3) The Google Wallet Privacy Policy states that it only shares information with third parties like developers as permitted under the Google Privacy Policy or as necessary for transactions.

a. What is the process for the consumer to obtain notice in this statement or in the Google Privacy Policy?

Prior to making a purchase on Google Play, buyers are required to sign in to their Google Account and activate Google Wallet. The buyer is presented with a link to the Google Wallet Privacy Notice and Terms of Service. We disclose in the Wallet Privacy Notice that we may share your personal information as necessary to process your transaction and maintain your account.

Google Wallet also sends a receipt to the user's registered email address under the Google Play name immediately following every purchase. The email receipt informs the user that a purchase has been made on Google Play and identifies the item purchased, the developer from whom the item was purchased, and the price. The receipt states very clearly: "You've made a purchase from [app developer] on Google Play." The email receipt includes links to the user's order history on Google Play, the Help Center, and the Google Play Refund Policy. The notice also provides a link that facilitates user contact directly with the app developer in the event of any questions or confusion about the bill.

We are always looking for ways to better explain our practices to users (buyers and merchants alike), which may include giving users a better understanding of how the online payments ecosystem works.

b. Is there a moment during purchasing an app where they learn that their address is disclosed as part of purchasing an app through Google Play?

Buyers are required to agree to the Wallet Privacy Notice prior to making their first purchase on Play. We disclose in the Wallet Privacy Notice that we may share the buyer's personal information as necessary to process her transaction and maintain her account.

c. Was this also the policy for payment processing before Google Play?

We have disclosed in the Wallet Privacy Notice since 2006 (prior to the launch of Google Play or Play's predecessor, Android Market) that we may share personal information with third parties as necessary to process your transaction and maintain your account.

(4) The Google Wallet Privacy Policy states that Google is not responsible for how developers or other third parties choose to use or share consumer information.

a. What precautions does Google take to avoid harmful uses of the consumer's data by third parties?

Google Wallet does not share users' full credit card or payment credential information with developers or other merchants using Google Wallet. This allows buyers to purchase digital goods online without sharing full payment details typically required for digital goods purchased directly from the merchant.

Any misuse of the customer information merchants do receive would be a violation of our terms. Google Play developers are required to agree to the Play Developer Distribution Agreement (see Section 4.3) and the Seller Terms of Service (see Section 7.1), which require developers to protect the privacy and confidentiality of buyers' personal information. Our Program Policies and Guidelines also provide strict instructions on communicating with buyers, and prohibit selling or renting buyers' information or sending marketing emails

to buyers without consent. Beyond the Google Play agreement, all merchants must also comply with local privacy laws.

We also take steps to prevent publication of potentially harmful apps. After the developer uploads its apps to the store but before they are made available to users on Google Play, Google automatically scans all apps for potentially harmful software with another risk engine. If potentially harmful software is identified, the security team prevents the app from publication and bans the developer from future use of the system. If the risk engine does not detect potentially harmful software, the developer may publish the app, which becomes available to users. While app downloads doubled during 2011, potentially harmful app downloads decreased by 40% for the same period.[2]

b. Are there any mechanisms in place to mitigate the exploitation of data by third parties?

As mentioned above, misuse of customer information would be a violation of our terms. Our Program Policies and Guidelines also provide strict instructions on communicating with buyers, and prohibit selling or renting buyers' information or sending marketing emails to buyers without consent. When app developers violate these terms, Google has taken administrative actions ranging from issuing warnings to suspending the developer.

Google Wallet does not share users' full credit card or payment credential information with developers or merchants using Google Wallet.

As mentioned above, Google Play automatically scans apps for potentially malicious software.

We hope these responses to your specific questions address any concerns you may have. However, please let us know if you would like to discuss this further.

Sincerely,

Susan Molinari
Vice President, Public Policy and Government Affairs
Google, Inc.

[2] More details available in our blog post from February 2, 2012: http://googlemobile.blogspot.com/2012/02/android-and-security.html