Feb. 25, 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:

I am writing on behalf of Consumer Watchdog, a nationally-recognized nonprofit consumer education and advocacy organization, to formally lodge a complaint about Google's most recent egregious privacy violation – the disclosure of confidential user information to independent application developers – and to request immediate Commission action to rectify Google's conduct and to compel Google's future adherence to the law and to its obligations under the "Buzz Consent Order." As explained below, Google should face penalties into the billions of dollars.

You will recall that Consumer Watchdog challenged in federal court the FTC's most recent privacy settlement with Google over that company's violation of the "Buzz Consent Order." We refer to that most recent FTC privacy settlement with Google as the "Safari Hacking Settlement." In its court papers, Consumer Watchdog argued that the Safari Hacking Settlement was inadequate to deter future Google violations of the Buzz Order because the settlement lacked a court injunction proscribing future violations, contained an express denial of liability by Google, and imposed a manifestly inadequate civil penalty.

In the face of this criticism, the Commission stated that "the most important question is whether Google will abide by the underlying [Buzz] FTC consent order going forward."[1] The Commission stated its "firm belief" that the $22.5 million fine would "promote such future compliance [with the Buzz Order]."[2] In its court papers, the FTC claimed that the paltry fine would "remove any economic incentive for similar [Google] conduct in the future."[3]

To no one's surprise (and the Commission's prior statements notwithstanding), the press is now awash in reports that Google has violated the Buzz Order yet again – and this time in a most substantive and egregious manner, by giving personal and closely held information from

[1] Statement of the Fed. Trade Comm., *In the Matter of Google Inc.*, FTC Docket No. (-4336 (August 9, 2012).

[2] *Id.*

[3] United States' Response to Consumer Watchdog's *Amicus Curiae* Brief (September 25, 2012) at 10.

tens (if not hundreds) of millions of Android users to independent and unrestrained application developers, in contravention of Google's own stated privacy policy (as well as its obligations under the Buzz Order). This represents the fifth significant misuse of confidential user data by Google in the last three years (previously, the "Wi-Spy" scandal, the Google Buzz fiasco, Google's improper combining and use of personal data, and the Safari Hacking episode).

To reiterate, with this letter we formally lodge a complaint about Google's most recent Buzz Order violation – the disclosure of confidential user information to independent application developers. We request immediate Commission action to rectify Google's conduct and to compel Google's future adherence to the law and to its obligations under the Buzz Order.

We briefly recount below Google's previous mishandling of confidential user information and the Commission's halting efforts to police Google's conduct. We then explain Google's current actions in transmitting confidential user data outside of its own company in violation of its stated privacy policy. Then, using readily available public data, we calculate the appropriate civil penalty that should be imposed on Google under the relevant statutes.

Obviously, if the Commission takes its obligation to protect the privacy of consumers seriously – and if the Commission expects Google (or the public at large, for that matter) to take the Commission's enforcement function seriously – then the Commission needs to adopt a new and different approach toward Google's violations. The strategy of initiating enforcement procedures by proposing a settlement followed by secret negotiations and a toothless decree has brought the Commission little beyond public condemnation. And consumers have not been protected adequately by the Commission's enforcement actions.

We now know from the Bartley Declaration filed by the FTC in the Consumer Watchdog case that the Commission staff initiated enforcement proceedings in the Safari Hacking episode by proposing a settlement.[4] We suggest, this time around, that the Commission begin its enforcement procedure by assigning a team of trial litigators – people who can actually conduct a trial – to the latest Google transgression and that these lawyers actually bring suit in federal court against Google for the latest violation of the Buzz Order. The complaint should seek injunctive relief sufficient to enforce compliance to the Buzz Order through contempt actions, as well as an appropriate civil penalty – which, as we explain below, will run into the billions of dollars.

This approach will actually position the Commission to secure something meaningful through negotiations. And, if Google refuses to settle on a meaningful basis, then the public will benefit from the trial disclosure of Google's misconduct. Most importantly, this approach will restore some integrity to the Commission's procedures.

[4] Declaration in Support of United States' Response to Consumer Watchdog's *Amicus* Brief (filed September 28, 2012) at ¶¶ 2-4.

**Google's Prior Privacy Breaches**

**Wi-Spy Scandal:** As part of the "Street View" feature of its mapping service, Google deployed fleets of cars outfitted with cameras to collect photographs of street scenes, including private homes. After repeated denials, Google finally admitted that its cars had collected entire texts of emails and passwords from Wi-Fi access points.

Important members of Congress, as well as Consumer Watchdog, requested that the FTC conduct an investigation. But no formal investigation was ever undertaken; no charges (either in the FTC or in the courts) were filed; no order to regulate future conduct was entered; no fines were assessed. Instead, the then-director of the Bureau of Consumer Protection ended his informal inquiry on the basis of Google's representations that it would change its internal policies to protect user privacy.

**Google Buzz:** Google launched a social networking service called Buzz in February 2010, by taking personal information provided by registered users of Gmail and integrating that information into Buzz without user permission and contrary to Google's written privacy policy at the time. Once again, members of Congress called for "a careful investigation."

On March 20, 2011, the FTC published a consent agreement with Google that contained no fine. Rather, the settlement barred Google from certain privacy misrepresentations, required Google to implement what the FTC called a "comprehensive privacy program," and mandated regular, independent privacy audits. "This is a tough settlement that ensures that Google will honor its commitments to consumers and build strong privacy protections into all of its operations," stated the FTC Chairman in a press release.

**Combining Personal Information:** On January 24, 2012, Google announced that it would implement changes to its user policies. Under the new policies, Google would "combine personal information from one service with information, including personal information from other services" without obtaining user permission. Numerous countries opened investigations into Google's policy changes but the FTC took no action at all, despite an inquiry from the co-chairman of the Congressional Bi-Partisan Privacy Caucus.

**Safari Hacking:** On February 17, 2012, the *Wall Street Journal* published a story alleging that Google had been using "special code" that "tricks" Apple's Safari web-browsing software, permitting Google to track "the Web-browsing habits of people who intended for that kind of monitoring to be blocked."

On April 8, 2012, the FTC (represented by the Department of Justice) filed a complaint in federal court charging that Google's conduct in bypassing Safari's privacy settings violated the Buzz Consent Order. Simultaneously with the filing of the complaint, the FTC filed a motion for court approval of a settlement with Google that provided only for a civil penalty of $22.5 million and a requirement that Google maintain for a few months systems to "expire" tiny tracking files it had placed on user computers without permission.

As we indicated above, despite a torrent of criticism, the FTC publicly contended that the settlement provided "a strong message to Google" that the "Commission will respond to

violations quickly and vigorously."[5] A federal district court dismissed Consumer Watchdog's challenge to the adequacy of the settlement based upon the Commission's representations.

**Google's Most Recent Misconduct**

There were 500 million Google Android devices (*e.g.* smartphones, tablet computers) activated as of September 11, 2012.[6] Most Google services require users to sign up for a Google account. Users must provide Google with personal information including the user's name, email address, telephone number and credit card.[7]

Google's general Privacy Policy[8] promises to keep this information confidential. Specifically, under the heading "Information we share," the policy states

> We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances apply.

The Policy then lists four such "circumstances": "With your consent," "With domain administrators," "For external processing," and "For legal reasons."

Users perform functions with their Android devices largely through applications that they purchase (or download for free) from the Google application store, known as "Google Play." A user needs a Google account in order to download apps from Google.[9] Only seven percent of Android smartphone users have never purchased an app; 19% of Android smartphone users have reportedly purchased more than twenty paid apps.[10] As of September 26, 2012, users had downloaded more than 25 billion apps from the Google Play store.[11]

The Google Play Terms of Service do not indicate that user data will be shared outside of Google, except with magazine publishers under certain specific circumstances.[12] But the Google Play Terms of Service (at heading 2) requires each user to set up and use a Google Wallet Account to purchase apps. And the Google Wallet privacy policy permits the sharing of user data outside of Google in only three narrow circumstances:

> We will only share your personal information with other companies or individuals outside of Google in the following circumstances:

---

[5] Commission Statement at 2.

[6] Hugo Barra, Google employee on Google+ https://plus.google.com/110023707389740934545/posts/R5YdRRyeTHM

[7] Google Privacy Policy, http://www.google.com/policies/privacy/

[8] *Id.*

[9] http://productforums.google.com/forum/#!topic/gmail/Pyhe926NfyI

[10] "Android catching up with iPhone on paid apps," Swiftkey, http://www.swiftkey.net/en/blog/android-catching-up-with-iphone-on-paid-apps/

[11] Google Play store hits 25 billion downloads, launches discount, http://news.cnet.com/8301-1023_3-57520324-93/google-play-store-hits-25-billion-downloads-launches-discounts/

[12] Google Play Terms of Service, heading 10, http://play.google.com/intl/en_us/about/play-terms.html

- 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.[13]

On February 13, 2013, the press began to report that Google had been sending to app developers personal information about each user who purchased an app from Google, without obtaining the user's permission. The personal information sent by Google specifically included the users' names, certain physical address information and email addresses.[14] According to the press, neither Apple nor Microsoft had engaged in similar conduct.[15]

Google's conduct constitutes a most serious breach of user privacy. Google Play apps deal with sensitive personal subjects, including health conditions and sexual activity. By disclosing personal user information to app developers, Google enables the identification of people who downloaded apps such as:

- **Depression App Counselor:** an app designed to help people suffering from depression to manage their symptoms.[16]
- **Pregnancy+:** an app for expectant parents.[17]
- **Heart Disease:** an app for people concerned that they are at risk of heart disorders.[18]
- **Utoopi:** a former app (now removed) "used for the purposes of advertising, soliciting and recruiting sex workers."[19]

Many Google app developers are young people. Google's disclosure of personal user information to these developers makes it possible for them to further disseminate the information. App developers can, for example, sell lists of customers to marketing services and data brokers – who will, in turn, sell the information to others.

The various applicable Google privacy policies promise not to share user information collected by Google outside the company. The policies contain no exceptions that would justify Google's disclosure to app developers of confidential user information. To date, Google has offered only a single defense to its conduct, and this through an unnamed company representative, who stated:

---

[13] Google Wallet Privacy Notice, http://wallet.google.com/files/privacy.html

[14] Google Play privacy slip-up sends app buyers' personal details to developers, http://www.zdnet.com/google-play-privacy-slip-up-sends-app-buyers-personal-details-to-developers-7000011249/

[15] Google raises new privacy concerns with app store policy, http://articles.chicagotribune.com/2013-02-14/news/chi-google-raises-new-privacy-concerns-with-app-store-policy-20130214_1_google-wallet-apple-inc-s-safari-privacy-practices

[16]https://play.google.com/store/apps/details?id=air.com.asdspecialist.depression&feature=search_result#?t=W10

[17] https://play.google.com/store/apps/details?id=com.hp.pregnancy&feature=search_result#?t=W10

[18]https://play.google.com/store/apps/details?id=com.onlinewerkz.heartdisease&feature=search_result#?t=W10

[19] See, Jane Hamsher, "Bytegeist Exclusive: Rep. Maloney Letter Blasting Google's Larry Page Over Android Sex App Marketed to Students," http://bytegeist.firedoglake.com/2012/09/18/bytegeist-exclusive-rep-maloney-letter-blasting-googles-larry-page-over-android-sex-app-marketed-to-students/

> Google Wallet shares the information necessary to process a transaction, which is clearly spelled out in the Google Wallet Privacy Notice.[20]

As indicated above, the Google Wallet privacy policy contains an exception permitting the sharing of user information outside the company "as necessary to process your transaction and maintain your account." This exception is not even referenced in the Google Play privacy policy.[21] Even assuming it applies to Google Play transactions, it does not justify Google's sharing of user information with developers. Simply put, the shared information is not "necessary" to process user transactions. As various press reports indicate, user transactions are routinely processed without developers even being aware of their access to user information, much less needing it. Indeed, developers have stated to the press that they do not want and should not have this user information.[22]

Google's conduct violates Section 5 of the FTC Act (and analogous state laws) by misrepresenting the extent to which the company shares personal user information with third parties. Google's conduct also violates the Buzz Consent Order. That Order prohibits Google from misrepresenting "the extent to which [it] maintains and protects the privacy and confidentiality of any covered information." "Covered information" is defined to include information Google collects from an individual including "first and last name," "email address," and "physical location" – precisely the information Google is improperly disclosing to app developers. Buzz Consent Order, Part III.[23]

Proving Google's violation of the Buzz Order appears straightforward. As to the monetary amount of Google's liability, Section 5(l) of the FTC Act provides for a civil penalty in the amount of $16,000 for each misrepresentation to the many tens of millions of users who downloaded hundreds of millions of Google apps.

In the Consumer Watchdog Safari Hacking case, the Commission defended the small size of the proposed civil penalty on the grounds that a "per violation" calculation was "difficult to arrive at with any precision." Here, such excuses will not stand. The misrepresentation is public and ongoing; the number of downloads is known; the number of users who have purchased or

---

[20] Jessica Guynn, "Google draws fire over data sharing on app store," http://articles.latimes.com/2013/feb/16/business/la-fi-google-privacy-20130216

[21] In an FAQ on a Google Wallet website for developers, Google notes that it may share certain user information with a merchant, presumably to enable merchants to process payment. This disclosure appears on a site for app developers, not consumers. See Google Developers, Google Wallet for Online Commerce, Product FAQs, https://developers.google.com/commerce/wallet/online/faq

[22] *See, e.g.,* Dan Nolan, Massive Google Play Privacy Issue, Internet Hugbox (Feb. 13, 2013), http://phetdreams.tumblr.com/post/42959902001/massive-google-play-privacy-issue; Jessica Guynn, Google Under Fire for Sending Users' Information to Developers, L.A. Times (Feb. 14, 2013), http://www.latimes.com/business/technology/la-fi-tn-google-under-fire-for-sending-users-information-to-developers-20130213,0,7558815.story

[23] Apart from any privacy policy, the Buzz Order also requires Google to obtain affirmative consent from users before any "new or additional sharing" by the company of user information with a third party that would be a change from "stated sharing practices in effect at the time [Google] collected [user] information." Buzz Consent Order at II. Google never disclosed to users its sharing of confidential information, much less obtained their consent.

received downloads is known. Calculating the amount of the penalty is a simple matter of multiplication. The number is enormous (in the billions of dollars), and only a penalty of that magnitude will deter Google from future violation of the Buzz Order.

We therefore ask that the Commission move promptly – before Google can destroy relevant data – and effectively to enforce its prior order.

Respectfully submitted,

John M. Simpson
Privacy Project Director

cc: Chairman Jon Leibowitz, Commissioner Julie Brill, Commissioner Edith Ramirez, Commissioner Maureen K., Ohlhausen, Commissioner Joshua D. Wright and California Attorney General Kamala Harris