UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection

[date]

BY ELECTRONIC MAIL

[App Developer]

Dear Sir or Madam:

You currently offer a mobile application for download in the Google Play store. We are writing to you today because of code included in the application that may allow third parties to monitor consumers' television viewing for ad targeting or analytics.

We recently discovered that your mobile application "_____" includes a software development kit created by the company Silverpush. Silverpush makes available for application developers a "Unique Audio Beacon" technology that enables mobile applications to listen for unique codes embedded into television audio signals in order to determine what television shows or advertisements are playing on a nearby television. This functionality is designed to run silently in the background, even while the user is not actively using the application. Using this technology, Silverpush could generate a detailed log of the television content viewed while a user's mobile phone was turned on.

The Silverpush code embedded in "_____" appears similar to the code published by Silverpush in the Google Play store as a demonstration of its audio beacon technology. For example, the code is configured to access the device's microphone to collect audio information even when the application is not in use. Moreover, your application requires permission to access the mobile device's microphone prior to install, despite no evident functionality in the application that would require such access.

Upon downloading and installing your mobile application that embeds Silverpush, we received no disclosures about the included audio beacon functionality — either contextually as part of the setup flow, in a dedicated standalone privacy policy, or anywhere else.

For the time being, Silverpush has represented that its audio beacons are not currently embedded into any television programming aimed at U.S. households.[1] However, if your application enabled third parties to monitor television-viewing habits of U.S. consumers and your statements or user interface stated or implied otherwise, this could constitute a violation of the Federal Trade Commission Act.[2] We would encourage you to disclose this fact to potential

[1] Thomas Fox-Brewster, *Meet the 'Ultrasonic' Tracking Company Privacy Activists Are Terrified Of*, FORBES, November 16, 2015, http://www.forbes.com/sites/thomasbrewster/2015/11/16/silverpush-ultrasonic-tracking/.
[2] Specifically, Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce.

customers, empowering them to make an informed decision about what information to disclose in exchange for using your application. Our business guidance "Marketing Your Mobile App: Get It Right From The Start" can provide additional guidance on how to make sure consumers understand your data collection and sharing practices.[3]

Commission staff will continue to monitor your mobile application in the coming months and would encourage you to contact Kristin Cohen, Senior Attorney in our Division of Privacy and Identity Protection, if you have questions or have additional information about your privacy practices and disclosures. Kristin can be reached at (202) 326-2276 or kcohen@ftc.gov.

Sincerely,

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection

[3] Marketing Your Mobile App: Get It Right From The Start, *available at* https://www ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf.