EXHIBIT 5

**Analysis of Infringement of U.S. Patent No. 8,266,296 by United Parcel Service of America
and United Parcel Service, Inc.
(Based on Public Information Only)**

Communication Interface Technologies, LLC ("CIT") provides this preliminary and exemplary infringement ana infringement of U.S. Patent No. 8,266,296, entitled "*Application-Layer Evaluation of Communications Received By a M* patent") by United Parcel Service of America, Inc. and United Parcel Service, Inc. ("UPS"). The following chart illustra regarding infringement by UPS's commercial mobile device application(s) including the UPS Mobile App, UPS Go App App, along with any hardware and/or software for provisioning that mobile device application (collectively, the "Accuse information and belief, the exemplary version herein and previous versions of the Accused Instrumentalities distributed patents-in-suit operated materially in the same manner.

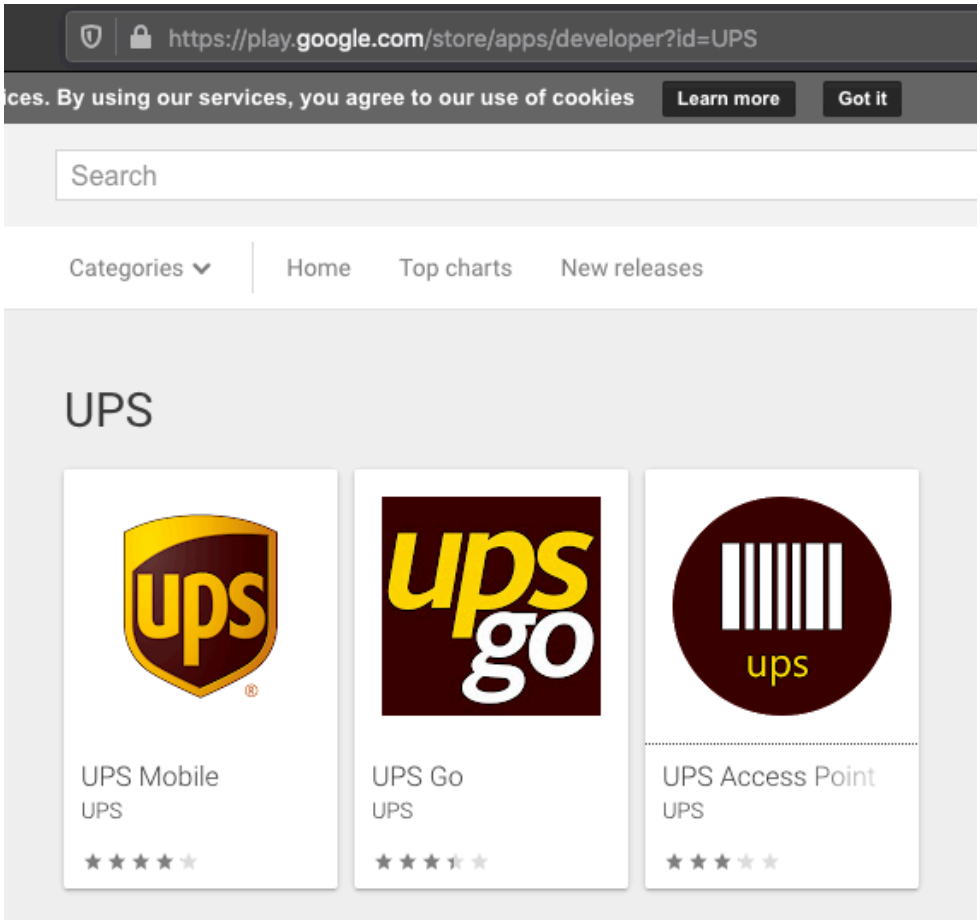
The analysis set forth below is based only upon information from publically available resources regarding the Ac UPS has not yet provided any non-public information.

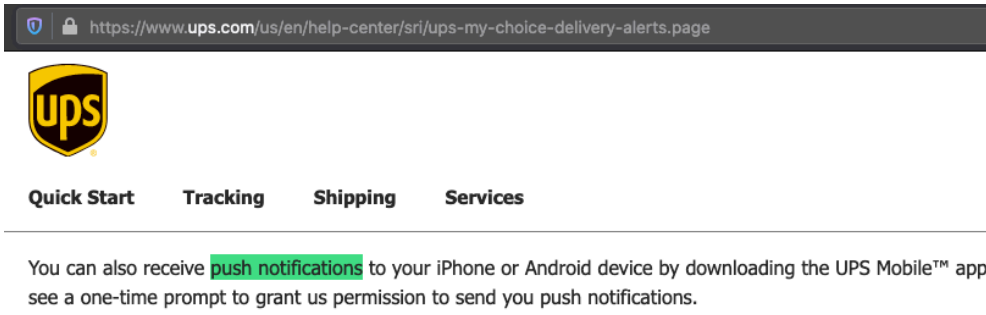
Unless otherwise noted, CIT contends that UPS directly infringes the '296 patent in violation of 35 U.S.C. § 271 making, using, and/or importing the Accused Instrumentalities. The following exemplary analysis demonstrates that inf

Unless otherwise noted, CIT believes and contends that each element of each claim asserted herein is literally me the Accused Instrumentalities. However, to the extent that UPS attempts to allege that any asserted claim element is not and contends that such elements are met under the doctrine of equivalents. More specifically, in its investigation and an Instrumentalities, CIT did not identify any substantial differences between the elements of the patent claims and the corr Accused Instrumentalities, as set forth herein. In each instance, the identified feature of the Accused Instrumentalities p the same function in substantially the same way to achieve substantially the same result as the corresponding claim elem

CIT notes that the present claim chart and analysis are necessarily preliminary in that CIT has not obtained subst nor has UPS disclosed any detailed analysis for its non-infringement position, if any. Further, CIT does not have the ben expert discovery. CIT reserves the right to supplement and/or amend the positions taken in this preliminary and exempl including with respect to literal infringement and infringement under the doctrine of equivalents, if and when warranted obtained by CIT, including but not limited to information adduced through information exchanges between the parties, f construction, expert discovery, and/or further analysis.

Analysis of Infringement of U.S. Patent No. 8,266,296 by United Parcel Service of America, Inc. a
(Based

	Claim 1	**UPS Downloadable App Service**
1	A method comprising:	A method is specified for controlling a virtual session on a user device such a *See https://play.google.com/store/apps/developer?id=UPS* 
1a (i)	receiving, at a control program executing on a mobile handset, a first communication initiated	Wireless push notification messages are sent over Transport Layer Security (message includes an encrypted push token as per Endnote #1. The push toke Notification message over TLS sessions from the UPS Server backend to the

	by a remote entity,	program, application layer program) running on a user's smartphone (mobile In the UPS application, for example, a push notification contains information *See https://www.ups.com/us/en/help-center/sri/ups-my-choice-delivery-alerts*  As per Endnote #1, the remote server causes a push notification message to b handset. Part of this push notification message (first communication) will be running on the user's smartphone or tablet device.
1a (ii)	wherein the first communication includes a set of information identifying an application layer program that is installed on the mobile handset, and	See Endnote #1 for a discussion of how each Push Notification message com includes an app-specific device token. The app-specific device token is indic running on the user's smartphone or tablet. Each incoming wireless push no an app-specific device token which is a set of information that identifies the process portion of the UPS App.
1a (iii)	wherein initiation of the first communication by the remote entity was not in response to a request sent by the mobile handset;	The message sent by the server is called a push message or a push notificatio call-out type messages, and as such, are not sent in response to pull requests *See* Endnote #1.
1b	the control program causing the mobile handset to evaluate the set of information included in the first communication; and	The control program is connected to the phone's OS that evaluates the first c the app-specific device token. This lets the system know which App on the the new incoming information to.

		See Endnote #1 for a discussion of how each Push Notification message com includes an app-specific device token. The app-specific device token is indi running on the user's smartphone or tablet. When the push notification has App, the UPS App provides user interface capabilities that allow the user to information received in the push message payload. When the user clicks thi evaluates this information and causes the UPS App to launch.
1c (i)	in response to determining, based on the evaluating, that the set of information identifies the application layer program, the control program causing the mobile handset to:	Determining is performed, for example, when a user clicks on a banner notif icon in the notifications tray. This determining is based on the evaluating, be at the app-specific device token and identifies the incoming push notification application program on the handset.
1c (ii)	launch the application layer program; and	Upon this determining, the user clicking of the notification icon in the banne the UPS App was launched during testing.
1c (iii)	reactivate, from an inactive state, a communication session between the mobile handset and the remote entity.	The Server Application and the client-side App have already established a se traditional client-server communications. For example the UPS Application session to communicate application data with the UPS App. Also in response to the user-clicking of the notification message and launchi other user interface selections provided in response thereto, the TLS session Application Server program and the UPS App is resumed. *See* Endnote#2 for a discussion of TLS session resumption. *See also*, *https:/ us/windows/desktop/secauthn/tls-handshake-protocol.* The remote server and the UPS application will resume their client-server TL and the remote unit can resume communications. To do so the application pr protocol stack within the remote unit to communicate back to the server via t TLS session use a full handshake sequence that is used to establish connectio abbreviated handshake sequence that is used to resume the TLS session from to an active state whereby new payload data can be sent via the virtual sessio

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.