BLU
BOLD LIKE US

10814 NW 33rd ST Miami, FL 33172 | T: 305.715.7171 | F: 305.436.8819 | E: sales@bluproducts.com | www.bluproducts.com

August 1, 2017

Dear Valued BLU Consumer:

Our consumers are the core of our beliefs and BLU is devoted in continuing to work tirelessly towards ensuring that we meet and exceed your expectations. We are all one team, a family with a common purpose – to provide the best-in-class design, quality and affordable mobile phones in the global market. As BLU launches our products to the consumers in Japan, we would like to share the following statement with you, to put at ease any privacy concerns you may have regarding our products, below is a full explanation of our actions.

BLU Products would like to confirm the smartphone devices being sold in Japan, the Grand M and Grand X LTE does not use Adups and is currently using Google Over the Air (GOTA) system. In addition, the Mediatek logger v4.2.0 and above is approved by Google to be used on any smartphones submitted for approval, has been cleared of any vulnerabilities by Mediatek and Google.

BLU Products responded to inaccuracies reported by several news outlets making clear that there is absolutely no spyware or malware or secret software on BLU devices, these are inaccurate and false reports. BLU is reaching out to several reporters to correct their articles and issue apologies, which BLU has started receiving.

The original report by Kryptowire issued on November 2016 regarding the Adups OTA application, stated a small fraction of BLU phones had a version of the application which was collecting phonebook contacts and text messages. Since BLU was unaware of this collection, they hadn't notified customers, thus it was deemed as a potential privacy issue. BLU moved quickly and resolved the problem by having Adups turn off this functionality.

Furthermore, BLU decided to switch the Adups OTA application on future devices with Google's GOTA. Even though it is BLU's policy to only use GOTA moving forward, some older devices still use ADUPS OTA.

Using ADUPS OTA is not an issue here. ADUPS is a well-known application used by several device manufacturers around the world. The issue is exactly what kind of data is actually being collected by this ADUPS application, and whether it presents a security or privacy risk.

BLU
BOLD LIKE US

10814 NW 33rd ST Miami, FL 33172 | T: 305.715.7171 | F: 305.436.8819 | E: sales@bluproducts.com | www.bluproducts.com

BLU hired Kryptowire in November of 2016 since their first report to regularly monitor the ADUPS application in their devices, and they have since been doing that. The data that is currently being collected is standard for OTA functionally and basic informational reporting. This is in line with every other smartphone device manufacturer in the world. There is nothing out of the ordinary that is being collected, and certainly does not affect any user's privacy or security. In addition, as per Tom Karygiannis, VP of Kryptowire, the data collection is in line with BLU's Privacy Policy, and does not constitute any wrong doing by BLU.

Regarding that some information may be stored in China servers, their privacy policy clearly states that some of the data collected can be stored in servers outside the US, there is absolutely nothing wrong with having a server in China. BLU management takes issue with the statement that any server in China is prone to risk while several other multibillion dollar companies and other mobile manufactures such as Huawei and ZTE use them.

BLU has several policies in place which takes customer privacy and security very seriously, and confirms that there has been no breach or issue of any kind with any of its devices.

My Best Regards and Thank You Very Much,

Daniel Ohev-Zion
CSO