KILPATRICK TOWNSEND SullivanStrickler

7 KEY TAKEAWAYS

Understanding the Intelligence on Smart Devices: Considerations & Tips for Collecting From & Reviewing Smart Device Information for Internal & Government Investigations

Kilpatrick Townsend's Adria Perez, Partner on the Government Enforcement & Investigations Team and Greg Freemyer, Director of Forensics and Disputes, SullivanStrickler on a recent KT Sound Bytes Episode discuss practical considerations and tips for collection and review. These days, smart devices often contain the most valuable information for internal and government investigations. Traditional corporate email may not provide the entire story.

Key takeaways from the episode include:

1. To make a device collection successful, it is important to determine where the relevant information could be located, such as on what kind of physical device or if the information could be in back-up or synchronization archives on the cloud.

2. Archives can include information that dates back further than what is on the physical device.

3. Common information sources on smart devices that are helpful for internal and government investigations include:
   - SMS;
   - MMS;
   - Messaging applications (which may also include audio files and money transfer information);
   - Notes;
   - Call logs;
   - Contacts; and
   - Geographical location information.

4. Devices have latitude & longitude trackers. Locations can be imbedded in photographs taken by the device. If the device connects to any cell tower or WiFi network, the smart device will have detailed information on where the device was at a specific time based on that connection.

5. Time stamps on messages may be in UTC time; not the time zone in which the user is

5

Time stamps on messages may be in UTC time; not the time zone in which the user is based.

After collection, obtain a spreadsheet with the device's various information sources along with snippets of the messages or notes found on the device. Use these snippets to determine which information sources should be reviewed and what search terms should be applied initially for a targeted review.

6

7

Messages provide a snapshot in time. In your review tool, you may only see a conversation between the same participants within 24 hours. In order to understand what occurred, including whether participants are added or taken off the message string, you will need to review the messages around the same time period, and possibly even create a chronology to avoid missing any key or related conversations.

For more information, please contact:
Greg Freemyer, gfreemyer@sullivanstrickler.com
Adria Perez, aperez@kilpatricktownsend.com

www.kilpatricktownsend.com