

The Prosecution Calls Your Smartphone to the Stand



Peter Silva, 2013-23-04

Or Bring-Your-Own-Defendant

A very real legal situation is brewing in the wake of the bring your own device phenomena. #eDiscovery. You might be familiar with some of the various [legal or liability issues that should be addressed](#) with a BYOD policy, like privacy, the loss of personal information, [working overtime](#) or the fact that financial responsibility may dictate legal obligation.

Now, technology law experts are saying that if your company is involved in litigation, criminal or civil, personal mobile devices that were used for work email or other company activity, could be confiscated and examined for evidence [as part of the investigation or discovery process](#). So if you use your personal smartphone for work related activities and your company is involved in a lawsuit, there may come a point where the court might subpoena your phone to see what relevant evidence might be contained. During litigation, the organization itself may have the legal obligation to sift through your mobile device for related information. If sued, companies are required to make a good-faith effort to retrieve data - where ever that may be. That includes your email, GPS history, text messages, cell phone records, social media accounts, pictures and any other info that could be pertinent to the case. This is proprietary company owned data that resides on my personally owned device. This is especially true of your corporate email co-mingles with your personal email - meaning delivered through the same email app or program. In fact, [according to this article](#), a judge recently sanctioned a company for a discovery violation because it did not search the BYOD devices during discovery.

Some people seem to lose all sense of daily human functioning when social networks like Facebook, Twitter and others are unavailable for a short period of time. We've become so attached to our mobile devices and they have become the center of our lives...imagine not having that pacifier for a few days. *OMG, I've time-traveled the 1980's and have no way of announcing it to the world!! What am I going to do now that I can't re-tweet that funny cat picture! I'm so lost without you, oh electronic appendage.*

As more organizations embrace or even require BYOD in the workplace, it becomes even more critical to be able to separate personal and work profiles. It is important that the corporate data and apps do not mingle with the already present personal data. Solutions like [F5's Mobile App Manager](#) provides a fully enclosed virtual enterprise workspace and creates a secure footprint on the device for enterprise data and access only. MAM allows organizations to safely separate personal data and usage from corporate oversight and controls how employees access key corporate information.

ps

Related:

- [Use your personal smartphone for work email? Your company might take it](#)
- [BYOD Lawsuits Loom as Work Gets Personal](#)
- [BYOD and Delta Airlines Privacy Lawsuit](#)
- [BYOD gets messy with AT&T class action lawsuit](#)
- [Is BYO Already D?](#)
- [BYOD Policies – More than an IT Issue Part 1: Liability](#)
- [BYOD Policies – More than an IT Issue Part 2: Device Choice](#)
- [BYOD Policies – More than an IT Issue Part 3: Economics](#)
- [BYOD Policies – More than an IT Issue Part 4: User Experience and Privacy](#)
- [BYOD Policies – More than an IT Issue Part 5: Trust Model](#)
- [BYOD 2.0: Moving Beyond MDM \(pdf\)](#)
- [Inside Look: F5 Mobile App Manager](#)

Technorati Tags: [ediscovery](#),[legal](#),[courts](#),[litigation](#),[byod](#),[discovery](#),[lawsuit](#),[policy](#),[liability](#),[silva](#),[f5](#),[mam](#),[mobile device](#),[smartphone](#)

Connect with Peter:

Connect with F5:



F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113