FBI FINALLY MOVES TO FIX ITS TEXT RETENTION PROBLEM — AND MOBILE PHONE SECURITY

Back when DOJ IG released a report explaining its efforts to ensure it had reconstructed all of Peter Strzok and Lisa Page's text messages, I pointed out that most people were missing the really important part of the story: FBI was making do with a vendor who — even after that scandal — still missed 10% of texts.

> And in trying to invent an obstruction claim out of normal bureaucratic thriftiness, they are ignoring the really damning part of the IG Report. The government contractor whose "bug" was responsible for the text messages that weren't originally archived (but which were later recovered) still can't ensure more than 90% of FBI's texts are recovered.
>
> > Among the other excuses FBI offers for implementing a fix to a 20% failure with one that still results in a 10% failure is to say, "complete collection of text messages is neither required nor necessary to meet the FBI's legal preservation obligations" (which goes back to how they're requiring retention via policy, but not technologically-assisted procedure). The FBI also says that it "is not aware of any solution that closes the collection gap entirely on its current mobile device platforms," which makes me

> > wonder why they keep buying new Samsungs if the Samsungs aren't serving their needs? Aside from the question of why we'd ask FBI Agents to use less secure Korean phones rather than more secure American ones (note, Mueller's team *is* using iPhones)?

This is a huge problem in discovery in criminal prosecutions. Just as an example, DOJ claims it didn't have texts between the Agents who were officially staking MalwareTech out in Las Vegas before they arrested him in 2017 and … other Agents. But if FBI doesn't actually competently archive those texts, how can they make that claim?

More troubling still, FBI didn't have a handle on what privileges their unnamed and squirrely data retention vendor had onto FBI Agents' phones.

> As DOJ IG was trying to puzzle through why they couldn't find all of Strzok and Page's texts, the unnamed vendor got squirrelly when asked how the retention tool interacts with administrative privileges.
>
> > Upon OIG's request, ESOC Information Technology Specialist [redacted] consulted with the FBl's collection tool vendor, who informed the FBI that the collection application does not write to enterprise.db. [Redacted] further stated that ESOC's mobile device team and the vendor believed enterprise.db is intended to track applications with administrative privileges and may have been collecting the logs from the collection tool or another source such as the Short

> > Message Service (SMS) texting application. The collection tool vendor preferred not to share specific details regarding where it saves collected data, maintaining that such information was proprietary; however, [redacted] represented that he could revisit the issue with the vendor if deemed necessary.
>
> Maybe it's me, but I find it pretty sketchy that this unnamed collection tool vendor doesn't want to tell the FBI precisely what they're doing with all these FBI Agents' texts. "Proprietary" doesn't cut it, in my opinion.

DOJ IG has now done what I was hoping they would: use the Strzok-Page incident as an opportunity to identify recommendations to fix the problem more generally. Most alarmingly, it says that the Subject Matter Expert it consulted in this process identified security vulnerabilities in its collection process.

> [D]uring the OIG's forensic examination of FBI mobile devices that were used by the two employees, the OIG discovered a database on the mobile devices containing a plain text repository of a substantial number of text messages sent and received by those devices.
>
> Neither ESOC nor the vendor of the application was aware of the existence, origin, or purpose of this database. OIG analysis of the text messages in the database compared to ESOC productions of text messages during the same time periods when the collection tool was functional identified a significant number of text messages found in the database that were missing from the ESOC production. Furthermore, the Subject

> Matter Expert with whom the OIG consulted in connection with its forensic analysis of the devices identified additional potential security vulnerabilities regarding the collection application. The OIG has provided these findings to the FBI.

Remember: these phones were used by people read into the most sensitive counterintelligence investigations. They weren't texting a lot about those investigations on those phones, but they were texting unclassified information about the investigations.

So now, two years after these texts were identified, DOJ's Inspector General is recommending that FBI fix what even I recognized was a security vulnerability — as well as the other, unnamed ones their SME identified.

> Coordinate with the collection tool vendor to ensure that data collected by the tool and stored on the device is saved to a secure or encrypted location.
>
> Verify and address the security vulnerabilities identified by the Subject Matter Expert with whom the OIG consulted, which have been provided to the FBI. Current and future mobile devices and data collection and preservation tools should be tested for security vulnerabilities in order to ensure the security of the devices and the safekeeping of the sensitive data therein.

Accused defendants should not have to guess whether or not the FBI Agents investigating them discussed their case via texts that have disappeared forever. And the country, generally, should not have to worry that the phone of its top counterintelligence Agent might be compromised because of a dodgy vendor FBI hired to collect (some of) his texts.

Sadly, DOJ IG doesn’t include another recommendation that seems like a no-brainer: that FBI switch to iPhones over the Samsungs they currently issue, both because iPhones have better security, but also because there is better visibility on the supply chain.