AFTER REPLACING FBI DEVICES TWO TIMES, THE BUREAU STILL FAILS TO COLLECT 10% OF AGENT TEXT MESSAGES

Today, DOJ's Inspector General released its report on the efforts it made to restore all of Peter Strzok and Lisa Page's text messages. The report is actually better used to illustrate how, three years into beginning to respond to its failures to collect all of the texts sent or received using FBI issued phones, and after twice upgrading the phones Agents get issued, it still fails to retain 10% of texts that Agents send and receive.

With regards to Strzok and Page, the report describes the efforts it made to obtain all their texts, which includes:

- Obtaining both the Samsung (Galaxy 5, then Galaxy 7) phones they used during this period, as well the iPhones issued for their brief stint in Mueller's office, the latter of which neither appears to have used
- Using the existing collection tool, which included big gaps for key periods of interest
- Asking DOD's Computer Forensic Lab for help
- Searching the Enterprise database, which found a bunch more texts, for

reasons no one could explain
- Hiring an outside Android consultant, who found 62 additional text messages

The upshot is, FBI doesn't know whether they recovered all Strzok and Page's texts, and doesn't know why they didn't, if in fact they didn't.

And we're only learning this because the two of them decided to conduct an extramarital affair on their FBI-issued devices while serving on the two most high profile investigations in recent FBI history.

Which raises the question: is this also true for Agents investigating defendants without the clout of Hillary Clinton or Donald Trump? If necessary, would the FBI be able to find their texts?

The answer is, maybe not.

Here's what this report says about FBI's retention rules, generally.

First, important texts are retained by policy, not (technologically-assisted) procedure. So the country's premier law enforcement agency ensures that important law enforcement related texts are retained by saying anything covering these topics must be retained.

- Factual information about investigative activity
- Factual information obtained during interviews or interactions with witnesses (including victims), potential witnesses, experts, informants, or cooperators
- Factual discussions related to the merits of evidence

- Factual information or opinions relating to the credibility or bias of witnesses, informants and potential witnesses; and
- Other factual information that is potentially discoverable under Brady, Giglio, Rule 16 or Rule 26.2 (Jencks Act)

But it's up to the Agents to do that. And if they don't for some reason, they're instructed to ask the Enterprise Security Operations Center if they retained them. But the ESOC is not mandated to retain texts. They happen to, but it's not tied to any mandate to retain substantive communications required to be saved by policy.

The ESOC has a tool, by a vendor whose name may not even appear in redacted form in this report, that "wirelessly collect[s] text messages sent to or from FBI-issued mobile devices."

As the FBI's response to this report reveals, the Bureau has known for some time that that tool didn't collect everything, because they've told the OIG that on two prior occasions.

> Prior to the OIG's investigation into the FBI's actions in advance of the 2016 election, during at least two unrelated investigations, one of which dates back to 2015, the FBI made the OIG aware of gaps in FBI text message collection capabilities.

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.

In any case, the FBI started trying to fix the problem, starting in 2016. At the time they started, they were losing 20% of the texts sent and received. After two upgrades of Samsung phones and a fix to a "bug" later, they're still not collecting 10%.

> During calendar year 2017, the FBI phased out use of the Samsung Galaxy S5 devices by its employees and replaced them with Samsung Galaxy S7 devices because of software and other issues that prevented the data collection tool from reliably capturing text messages sent and received via FBI issued Samsung Galaxy SS mobile devices. According to FBl's Information and Technology Branch, as of November 15, 2018, the data collection tool utilized by FBI was still not reliably collecting text

> messages from approximately IO percent of FBI issued mobile devices, which included Samsung S7s and subsequently issued S9s. By comparison, the estimated failure rate of the collection tool was 20 percent for the Samsung S5s.

The FBI's tech folks provided these explanations for why the tool by the unnamed vendor still doesn't work.

- In calendar year 2016 the collection application vendor reported a "bug" in a version of the collection tool which caused the application to stop collecting text message or log data- This application version was replaced by a newer version that corrected the issue in March 2017.
- Errors during the initial installation of the collection application, such as misconfiguration during setup.
- Errors in the collection application's ability to send text message data caused by software updates or operating system updates on the mobile device itself.
- Hardware errors, such as the device not being powered on, being located in a poor cellular signal area, or being located in an area with no cellular service.

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 story, like so many with the hoaxes that Republicans have ginned up to try to delegitimize the Mueller investigation, seems to be the big story, not what Strzok and Page sent themselves two years ago (the IG Report concluded the non-discoverable texts did not cover one subject area, so weren't by themselves suspect, and doubted either Strzok or Page had the technical capability to selectively destroy only incriminating texts).

The FBI is an agency that routinely demands that people respond to subpoenas by pulling all the relevant texts on a given subject. If you were to fail, they would be at least consider whether your failure to do so amounted to obstruction. But they don't guarantee they would be able to meet that same standard — they're happy with their 10% failure rate, apparently.

And while it is an interesting topic for Strzok and Page and Donald Trump's attempts to claim Witch hunt! it's the instances where criminal defendants are asking the FBI to search for relevant texts among agents (in just one example, MalwareTech asked the FBI for texts between Agents surveilling and then arresting him in Las Vegas, but got nothing) that I care about. Because if you only aspire to 90%

retention, and if you attribute any failure to do better to an individual Agent's failure to meet a policy (but how would you prove it, if the point is that a given text no longer exists to be discovered?), then you're pretty much ensuring that you can't fully comply with discovery requests from defendants.

Apparently, the FBI seems okay with that.