IS FBI STILL FLUFFING ITS ENCRYPTION NUMBERS?

Note: All the big civil liberties groups are fundraising "bigly" off of the election of Trump. If you are donating to them and are able, please consider supporting this work as well.

Update: I went back to the FBI spox who originally told me that the 13% number cited in August included damaged phones, to clarify that this more recent one did. It does not. Here's what he said:

> It is true that damaged devices are provided to CART and RCFL for FBI assistance, but the 886 devices in FY16 that the FBI was not able to access (which is the number that GC Baker provided last week), does not include those damaged devices. It includes only those devices for which we encountered a password we were not able to bypass.

"[T]he data on the vast majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant," FBI Director Jim Comey wrote in a response to a question from Senate Judiciary Committee Chair Chuck Grassley in January. Grassley had asked whether Comey agreed with New York District Attorney's Cy Vance's estimate — made in Senate testimony the previous July — that "when smartphone encryption is fully deployed by Apple and Google, 71% of all mobile devices examined…may be outside the reach of a warrant."

In Comey's very next answer, however, he admitted the FBI was still trying to quantify the problem. "FBI is currently working on improving enterprise-wide quantitative data

collection to better understand and explain the 'data at rest' problem." Comey and Deputy Attorney General Sally Yates had promised to come up with real data at the July 2015 hearing.

Since that time, FBI has publicly created the impression they had real numbers on encryption.

In a speech at the end of August, Jim Comey claimed that the FBI had been unable to open 650 of the 5,000 devices it got in its forensics centers (remember, the fiscal year starts on October 1).

> We believe in the FBI that we need a conversation. If at the end of the day the American people say, "You know what, we're okay with that portion of the room being dark. We're okay with"—to use one example—"the FBI, in the first 10 months of this year, getting 5,000 devices from state and local law enforcement and asked for assistance in opening them, and in 650 of those devices being unable to open those devices." That's criminals not caught, that's evidence not found, that's sentences that are far, far shorter for pedophiles and others because judges can't see the true scope of their activity.

That left the impression that encryption thwarted the FBI in 13% of all cases.

According to Kevin Bankston, FBI General Counsel just provided an equivalent number at a National Academy of the Sciences working group on encryption (Baker only said these were inaccessible — he did not claim that was because of encryption, though that was the context of the number).

> Interesting data point: Baker says over FY 2016, of 6814 mobile devices submitted by fed/state/local to FBI's [Computer Analysis Response Teams and Regional Computer Forensic Laboratories for analysis 2095 of them req'd

> passcodes, defeated passcodes in 1210 cases, unable to (presumably due to crypto?) in 886 (885?) cases.

That reflects the same 13% failure rate.

I asked the FBI in September where they got this number. And at least at that point, the 13% was not a measure of how often encryption thwarted the FBI. A spokesperson told me,

> It is a reflection of data on the number of times over the course of each quarter this year that the FBI or one of our law enforcement partners (federal, state, local, or tribal) has sought assistance from FBI digital forensic examiners with respect to accessing data on various mobile devices where the device is locked, data was deleted or encrypted, the hardware was damaged, or there were other challenges with accessing the data. I am not able to break that down by crime type.

In the San Bernardino case, for example, the FBI may not have been able to access 66% of the phones it seized from the culprits (there are actually varying reports on this). But in the end, encryption accounted for none of those phones being inaccessible: physical destruction accounted for all of it.

So unless the FBI, after I asked in early September, went back and recalculated their quarterly numbers (I've got a question in to clarify this point), then the FBI is presenting a false claim about encryption.