JEFFREY CLARK: PHYSICS TAKES OVER THE INVESTIGATION NOW

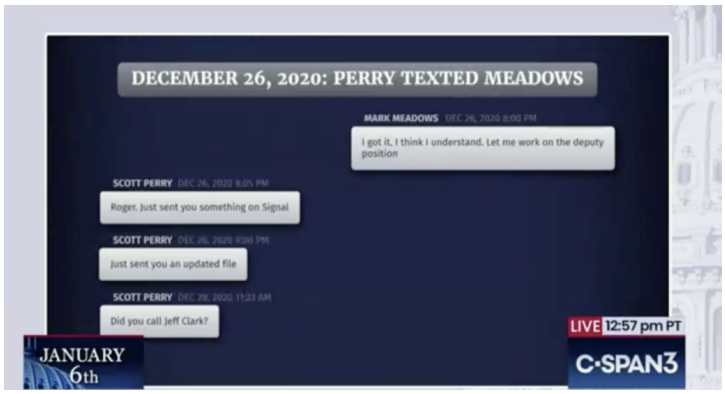
Last Thursday was an exciting day for those who have doubted Merrick Garland's DOJ was really investigating top officials for matters pertaining to January 6.

Not only did multiple outlets describe Republicans involved in the fake elector scheme receiving subpoenas or even, in at least three cases, search warrants for their devices, but Jeffrey Clark's home in Virginia was also searched on Wednesday. As part of that, according to the hysterical account Clark gave on Tucker Carlson, whatever agency did the search used an electronics sniffing dog and seized all the electronics in the house.

And that makes it a really good time to talk some more about how investigations work in the era of encrypted applications. It's likely to be months — likely at least six months — until anything comes out of last week's seizures.

The reason has to do with physics (and law).

We can be fairly certain *that* Clark — and probably some of the fake electors on whom warrants were served — used Signal or other encrypted apps. That's because Mark Meadows and Scott Perry were conducting some of this conspiracy over Signal too, as was made clear in a slide in Thursday's hearing.



Indeed, one reason Clark may have been raided is because he makes an easier target, for now, than Meadows or the Members of Congress who were involved. All of Clark's communications directly with then President Trump bypassed DOJ's contact guidelines and most can be shown to be part of a plot to overturn the election, whereas many of Meadows' communications will be protected by Executive Privilege and Perry's by Speech and Debate (though as I keep repeating, DOJ will be able to piggyback off the privilege review that the January 6 Committee has done).

To obtain Signal conversations that haven't been saved to the cloud, one needs at least one of the phones that was involved in the conversation. That assumes the texts were not deleted. In the James Wolfe investigation, the FBI demonstrated some ability to recover deleted Signal texts, but in the Oath Keeper investigation, their Signal deletions forced investigators to seize a whole bunch of phones to reconstruct all parts of the communications.

By law, the government should have some of these Signal texts accessible. Under the Presidential Records Act, Mark Meadows had a legal obligation to share any such texts with the Archives. But because he replaced his phone in the months after the insurrection, at a time he knew of the criminal investigation, he may not have been able to comply. If DOJ can prove that he deleted Signal texts, he might be on the hook for obstructing the DOJ investigation.

So one thing DOJ may have been trying to do, by seizing the phones of at least four players in

the fake electors plot on the same day, was to obtain phones sufficient to reconstruct any Signal threads about the plot. Those served subpoenas, both in this and an earlier round of subpoenas, will have to turn over Signal texts too, if they meet the terms of the subpoena. If DOJ were trying to reach the far higher bar of obtaining a warrant against someone protected by Speech and Debate or other privileges — like Perry — they likely would need to use such threads to meet that higher bar.

So back to the physics.

The table below shows how the investigations into a number of high profile investigative subjects have proceeded. While there are exceptions (investigations where the FBI has some excuse or urgency to conduct an interview, as with Mike Flynn and George Papadopoulos, are different), investigators often first obtain readily accessible cloud content with a gag order, then use the information from a person's cloud content to obtain probable cause for a warrant to seize phones. Under that pattern, the phone seizure will alert a subject of an investigation to that investigation. In most cases (the first round of January 6 arrests and Roger Stone are exceptions, each for different reasons), the search of phones precedes any arrest by months if not years.

Investigative Subject	Metadata Orders	Initial Cloud Warrant	Additional Cloud Warrants	Initial Phone Seizure	Delay	Arrest or Plea
Michael Cohen	6/21/2017	7/18/17	8/7/17	4/9/18	Filter then Special Master	8/21/18
			11/13/17			
			2/28/18			
			4/7/18			
Roger Stone	5/12/17	8/7/17	9/11/17	1/25/19	Witness interviews	1/25/19
			10/17/17			
			3/14/18			
			7/27/18			
			8/2/18			
			8/3/18			
			8/8/18			
			8/28/18			
Rudy Giuliani		11/4/19		4/28/21	Filter then Special Master	
Project Veritas	11/24/20	1/14/21	1/26/21	11/4/21	Filter then Special Master	
			3/6/21			
James O'Keefe			4/9/21	11/6/21		
Stewart Rhodes				~5/10/21	Volume	1/12/22
Enrique Tarrio				1/4/21	Jurisdictional, password, then filter	3/7/22

Whereas, during the Mueller investigation, the FBI could exploit phones in four months time, of late, it has been taking closer to six months to exploit cell phones, even without any kind of special review. Part of this delay is physics: if a person uses any kind of secure password, it takes the FBI time to crack that password (and

still more time if someone uses additional security features, as Enrique Tarrio did). In many cases, the DOJ will have to use a filter team to exclude data that is somehow privileged; in all cases, DOJ will then do a scope review, ensuring that the investigative team only gets material responsive to the warrant. When a special review is required, such as the attorney-client privilege review for Rudy or the "journalistic" review for Project Veritas, that process can take much longer. Because DOJ will have to conduct a fairly exhaustive filter review for an attorney like Clark, it might take closer to nine months to exploit the devices seized last week.

This pattern suggests several things about the investigation into Jeffrey Clark (and the fake electors). First, DOJ likely obtained their first probable cause warrants against Clark and the fake electors months ago, probably pretty close to the time (though hopefully before) Lisa Monaco confirmed the investigation into the fake electors in January. In Clark's case, an investigation may have come from a referral from DOJ IG. So contrary to what many outlets have reported, such as this example from James Risen at the Intercept, the searches of Clark and others are not proof that an investigation *is beginning* or that DOJ only recently established probable cause. Rather, they suggest DOJ has been investigating covertly for months, at least long enough to obtain probable cause that even more evidence exists on these phones.

But it's also likely that it will take DOJ some months — until Christmas at least — to exploit Clark's phone. This investigation will not move as quickly as you might think or hope that this point, and that's partly dictated by the constraints of cracking a password — math and physics.

All that said, several prongs of an investigation that could implicate Trump may be much further on. As I'll show in a follow-up (and as I've mentioned in the past), the

investigation into Stop the Steal is undoubtedly much further on than people assume given Ali Alexander's grand jury appearance last week. And the FBI has ways of getting content via the Archives, much as they obtained content from Trump's transition from GSA, that bypass pattern laid out above.

What the government had to have been able to prove before it searched Clark and others last week was not just that that had probable cause against those subjects, but that the cloud content otherwise available to them showed that aspects of the crime were committed using materials only available on people's phones, likely encrypted messaging apps.

Update: Several people have asked why there would be a privilege review for Clark's phone, since he would have been a government attorney through January 6. I'm not certain there would be, but if a warrant covered the time since January 6 (which I think likely given what DOJ has done with warrants elsewhere), then any lawyering he has done since he left would be privileged.

Update: As noted in comments, also on Wednesday, the FBI seized John Eastman's phone. The warrant is from DOJ IG, not DC USAO and bears a 2022 case number. DOJ IG opened an investigation into Clark in 2021, but perhaps something they saw in the Jan6 Committee hearings led to a new prong of the investigation, leading to this search? Given the squirreliness regarding what agency did the search of Eastman, I wonder if both these investigative steps were DOJ IG.

Background material

This annotated file shows the unsealed Mueller warrants, with labels for those warrants that have been identified.

This post shows how the Michael Cohen investigation started with Russian-related warrants in the Mueller investigation then moved

to SDNY, including a crucial detail about preservation orders for Cohen's Trump Organization emails served on Microsoft.

This post shows how the investigation into George Papadopoulos developed; his is the outlier here, in that overt actions took place closer to the beginning of the investigation — but in his case, DOJ used a series of informants against him to obtain information.

This post describes how Trump's team only discovered Mueller had obtained transition devices three months after Mueller obtained them, via Mike Flynn's statement of offense.

This post shows that the seizure of Roger Stone's phones with his January 2019 arrest was just one step in an ongoing investigation.

This post uses the Michael Cohen example to explain how the Rudy investigation might work.

This post shows how the investigation into Project Veritas developed.

This post shows how it took almost an entire year to crack Enrique Tarrio's password, with a filter team delaying access for another month.

This post describes how the sheer volume of Stewart Rhodes' Signal texts delayed his arrest.