

THE HE SAID, SHE SAID THAT MAY RENDER MALWARETECH'S ARRESTING AGENTS USELESS ON THE STAND AT TRIAL

Back when Marcus Hutchins (MalwareTech) moved to suppress the statements he made in his first custodial interview after his arrest, I suggested the challenge itself was unlikely to succeed, but that it would "serve as groundwork for a significant attempt to discredit Hutchin's incriminatory statements at trial."


While I still generally think the effort is unlikely to succeed (though it may never come to that, as I lay out below), an evidentiary hearing on the issue yesterday may have rendered both his arresting agents largely useless for testimony at trial.

As a reminder, Hutchins originally challenged his statements because:

- As a Brit, he couldn't be expected to understand that US Miranda works in the opposite way as British Miranda does without specific explanation
- He waived his Miranda rights after being arrested after over a week of partying at DefCon, and was exhausted and possibly high
- The FBI's own records were sketchy; they hadn't recorded that he had been

asked if he was drunk (but not high) until over four months after his arrest (yesterday we learned that 302 was dated December 8 or 9)

Then, just before the originally scheduled evidentiary hearing on April 19, the government told Hutchins that the multiple crossed out times on his waiver had not been corrected until at least five days after his arrest, something the FBI agent in question, Jamie Butcher, didn't formally explain anywhere.

Witness: 
Time: 11:08 am - 2:08 pm ~ 1:18 pm

Hutchins lawyers got a continuance to understand the implications of that; yesterday was the rescheduled opportunity to grill the FBI agents about when he was really Mirandized.

From the get-go, Hutchins attorney Brian Klein set a contentious tone for the hearing by suggesting at the outset that they might need to call one or the other of the prosecutors to testify to impeach the agents, something that almost never happens (for mostly good reasons). After some preliminaries in which judge Nancy Joseph laid out how she'd be assessing the issues, first Lee Chartier and then Butcher took the stand to explain how the post-arrest interview and subsequent paperwork had gone down.

Chartier, almost a stereotypical-looking FBI agent – tall and white, beefy, with a goatee – had the more experience of the two: he's been working cyber since 2011 and in 2016 Jim Comey gave him the Director's Medal of Excellence for being one of the top performing cyber agents. Still, he testified he had only done around 50 interviews, of which 20 were custodial interviews, over those years. Butcher, a short

white woman, has been at FBI nine years, moving from an admin position to a staff operations specialist to her current cyber special agent position, where she's been for three years. When prosecutor Benjamin Proctor walked her through her background, he didn't ask how many interviews, custodial or no, she had done, which given Chartier's surprisingly low number, probably means she's done very few interviews, particularly custodial ones. When Proctor asked about her involvement in this case, he described it as "becom[ing] involved in the investigation that resulted in arrest of Marcus Hutchins," which suggests a curious agency behind the investigation.

Between them, the agents described how they flew out to Vegas the night before the arrest. Surveilling agents tracked Hutchins as he went to the airport and got through TSA then sat down at a first class lounge. As soon as Hutchins ordered a drink that turned out to be Coke but that the agents worried might be booze, Chartier, wearing business casual civvies, and two CBP agents wearing official jackets pulled Hutchins away from the lounge, placed him under arrest and cuffed him in a stairwell inside the secure area, and walked him to a CBP interview room, where Chartier and Butcher Mirandized him, then interrogated him for 90 to 100 minutes.

Even in telling that story, Chartier and Butcher's stories conflicted in ways that are significant for determining when Hutchins was Mirandized. He said it took "seconds" to get into the stairwell and then to the interview room. She noted that the "Airport is rather large. Would have taken awhile." to walk from place to place (it was 36 minutes between the time Hutchins cleared TSA, walked to the lounge, ordered a Coke, and the time Chartier first approached Hutchins). There seems to be a discrepancy on how many CBP agents were where when (that is, whether one or two accompanied Chartier and Hutchins all the way to to the interrogation room). Those discrepancies remained in spite of the fact that, as Butcher

admitted, they had spoken, "Generally, about the interview, and Miranda, and making sure that we were on, that our facts were the same."

Chartier described that the CBP recording equipment in the room "wasn't functional that day," which is why they relied on Butcher pressing a record button herself, which she didn't do until (she said) Chartier started asking "substantive" questions, but after the Miranda warning.

It sounds like Chartier did most of the questioning and the dick-wagging, even though Butcher was the lead agent. He offered up the term "Liquid Courage" to describe Hutchins' description of having to drink to network. He gave Hutchins a list of 80 online monikers, of which Hutchins recognized a handful; "Vinny," who has shown up in public reporting on Hutchins' background, was apparently one of those, so he may actually be the co-defendant after all (or the informant the government is hiding). Chartier had Hutchins review a string of code; Hutchins only recognized that it listed Kronos (which is the first he figured out that's what the interview was about, and which is what the FBI claim he inculpated himself as the coder of Kronos is based off).

Chartier's more dominant role in the questioning is interesting given the dynamic yesterday. Butcher, who was questioned second, seemed to know her multiple fuck-ups on the basic parts of this interview (failing to note the Miranda time, starting the recording late, offering unconvincing claims about what she did when she realized she had entered the time wrong on the consent form) make her an FBI short-timer. I'd honestly be surprised if she were still at FBI by the time this goes to trial, if it does. At times, she seemed not to recognize the dangers of the answers she was giving. Chartier, on the other hand, has his Director's award career to protect, and perhaps for that reason was openly hostile and seemed ready to throw Butcher under the bus for the fuck-ups that had gotten him

sucked in.

Except it was Chartier's responses that seemed to reflect deceit, and it was Chartier that Brian Klein accused of lying. Chartier seemed to be aware that he had to ensure three details:

- That he explained to Marcus the circumstances of his arrest, which allegedly happened in the stairwell (I think it shows up in the 302, which Butcher wrote, but she wouldn't have witnessed it. Also, her response to the judge on how she reconstructed the time of the waiver hinted that there are other sources of time stamps she doesn't want to reveal – I bet there is surveillance footage from the stairwell).
- That WannaCry only came up at the end.
- That Hutchins should have known the interview was about Kronos.

Except even the prosecution made clear that's not what happened. Prosecutor Michael Chmelar described how Hutchins first realized the case was about Kronos when he was shown the code.

Do you recall certain point Hutchins asked if case was about Kronos, looking for developer. What did you respond. I said I don't think we're looking anymore. Our belief that Mr Hutchins was developer of Kronos.

Note, I suspect the full 302 will also show that

Chartier had absolutely no reason to make this claim, which is probably why within days of Hutchins' arrest it became clear the FBI had way oversold their proof from this interview that Hutchins had admitted to contributing to Kronos.

Also at issue is when Hutchins first got to see the arrest warrant, something that Chartier's testimony appears dodgy on. More importantly, Chartier's testimony did make it clear Hutchins started asking immediately what the arrest was about, and 30 seconds after the recording started (therefore, after he had just signed the waiver) he asked again. Except it wasn't until an hour later that Chartier explained that this stop wasn't about WannaCry, as Klein laid out.

It's not until 1 hour into the interview that they show him arrest warrant. Here's what happens. Chartier. What you'll hear him say, okay, well, here's the arrest warrant, and just to be honest. If i'm being honest with you this has absolutely nothing to do with WannaCry.

Plus, the arrest warrant apparently did not lay out the charges in the indictment, instead listing "conspiracy to defraud the US" as the crime (good old ConFraudUs!) which is remarkable for reasons I may return to if and when the warrant is docketed.

Effectively, the government explains that the reason they didn't arrest Hutchins until just before he boarded his plane is because they feared he'd dodge off, open a computer, and shut down the WannaCry sinkhole, re-releasing the global malware. (Yeah, that's dumb.) Everything they did they did because of WannaCry.

But it wasn't until an hour into their interrogation of Hutchins that they told him it wasn't really about WannaCry.

Frankly, I don't think this thing is going to trial. When Klein asked for more time, given what they discovered yesterday, before arguing

the suppression motion, Joseph said she had all the other motions briefed and she wanted to decide them together. As I have laid out, the 5 motions work together, showing (for example) that the CFAA charge is improper, but also showing that the government refuses to point to any computers that were damaged by the Kronos malware Hutchins wrote.

If she's thinking of all those motions together, then she's seeing how, together, they show how pointless this prosecution is.

But if not – if this case actually *does* go to trial – either one of these FBI agents will be very easy to impeach on the stand.

Update: Fixed spelling of Chartier's last name.

Update, 5/31: Turns out I had Chartier's last name right the first time, and have now fixed this back.

Update: In talking to a physical surveillance expert who followed the hearing, the stairwell may actually be one place in the secure space that wouldn't be on surveillance footage, with cameras instead capturing the entry and exit. If that's right, it would mean the stairwell is all the more curious a place to have some of the key events in this arrest and interrogation go down.
h/t D0