MALWARETECH'S JUDGE SEEMS MORE SYMPATHETIC TO HUTCHINS ABOUT THE INTENT OF PROSECUTION THAN THE LAW

JP Stadtmueller, the judge who will preside over MalwareTech (Marcus Hutchins') case, last week denied his pretrial motions to get his post-arrest interview and all the charges of his indictment thrown out. The order starts this way:

> On March 30, 2018, Hutchins filed a motion to suppress the statement that he made to Federal Bureau of Investigation ("FBI") agents immediately following his arrest, as well as any evidence the government may have obtained as a result. (Docket #55)

We are almost 11 months into the pre-trial process and we're virtually the same place we started. Just two things have happened in that time: the FBI Agents who arrested Hutchins had badly damaged their credibility, and Stadtmueller has given a read of how he views the case.

Stadtmueller scolds the already discredited FBI Agents for violating Federal Rule of

Criminal Procedure

As to the first issue, in ruling against Hutchins on his Miranda claim (which I've always suggested was a way to discredit Hutchins' incriminating comments at trial), Stadtmueller makes it clear he finds the conduct of the FBI agents problematic. He sides with Hutchins on the dispute whether Agent Chartier showed him an arrest warrant in a stairwell exchange that appears to have been improperly referenced in his 302.

> The Court notes that the agents' testimony is somewhat contradictory on this point. Chartier stated that they showed Hutchins the warrant before the interrogation was recorded. By contrast, Butcher stated that they first showed Hutchins the warrant over an hour into the interrogation. The recording of the interrogation suggests that Butcher is correct. Specifically, over an hour into the recording, Chartier says: "Okay. Well, here's the arrest warrant. And just to be honest—just to be honest, hey, now I'm going to tell you the truth…If I'm being honest with you, Marcus, this has absolutely nothing to do with WannaCry." The balance of the evidence strongly suggests that Hutchins was not shown the arrest warrant until over an hour into the interrogation.

More importantly, he criticizes the Agents for what he calls an "abject failure of the agents to abide by the Federal Rules of Criminal Procedure."

> At one point in the interrogation, he made a comment that showed that he did not realize he had even been indicted. There is no reason why the government could not have told him exactly why he was arrested, as he requested, and as was required of them by Federal Rule of

> Criminal Procedure 4(c), unless they were concerned that he would not be cooperative with them. There is certainly an element of deception to this set of events that the Court does not endorse.
>
> [snip]
>
> The Court is concerned by the abject failure of the agents to abide by the Federal Rules of Criminal Procedure 4(c), but their obvious interest in Kronos—including providing Hutchins with a string of code related to Kronos—leads the Court to conclude that there is not clear and convincing evidence that they acted with intent to deceive.
>
> [snip]
>
> Hutchins does not argue the effect of the violation of Federal Rule of Criminal Procedure 4(c)(3)(A), which governs execution of a warrant:
>
> > Upon arrest, an officer possessing the original or a duplicate original warrant must show it to the defendant. If the officer does not possess the warrant, the officer must inform the defendant of the warrant's existence and of the offense charged and, at the defendant's request, must show the original or a duplicate original warrant to the defendant as soon as possible.
>
> Few courts have had moment to consider whether a violation of this rule would warrant exclusion of evidence, though it certainly might, for deterrent purposes, if the violation compromised a substantive constitutional right and the officers acted bad faith. Bryson v. United States, 419 F.2d 695, 701–02 (D.C. Cir. 1969); Murray v. United States, 855 P.2d 350, 353–56 (Wyo.

> 1993); United States v. Hamilton, 2017 WL 9476881, at *5 (N.D. Ga. Jan. 3, 2017). However, Hutchins did not raise this issue, so the Court will not consider it. Additionally, even if his statements were excluded, it is likely that the physical evidence still would be admissible. See United States v. Patane, 542 U.S. 630, 637–38 (2004) (failure to give Miranda warnings requires suppression of voluntary statements, but does not require suppression of physical evidence acquired as a result of those voluntary statements).

Taking Stadtmueller's hint, Hutchins' lawyers have renewed their motion to suppress the statements on that ground, but it may be too late. Whatever happens, though, this adds to the list of the things the FBI agents whose credibility will be deployed to enter Hutchins' statements fucked up during his arrest. And that's before you get into their technical knowledge.

Stadtmueller shows sympathy for the stupidity of prosecuting the guy who killed WannaCry

Along the way, Stadtmueller seems to get how stupid prosecuting the guy who killed WannaCry is.

> However, Hutchins's recent triumph with WannaCry had vaulted him into the public eye as a "white hat" hacker. Thus, Hutchins could have been reasonably confused about the FBI's interest in him. In assessing whether he voluntarily waived his rights, some consideration

> must be given to the fact that white hat hacking is a complex and relatively novel field that can toe an already blurry line vis-à-vis online criminal activity. The agents did not tell Hutchins why he was under arrest, and did nothing to explain the nature of the charges against him until the end of his interrogation. Hutchins, who had no cause for concern regarding his role in WannaCry, and who had distanced himself from nefarious internet activity, cooperated.

And, having reviewed the interrogation, he seems to regard Hutchins' attempts to help the FBI Agents identify the real criminals they are pursuing as good faith.

> Almost eighty minutes into the recorded interrogation, the agents finally provided him with the warrant, and told him that it had "nothing to do with WannaCry." The interrogation continued for about twenty minutes after that. Throughout the remainder of the interrogation, Hutchins tried to be helpful but noted that he had been "out" of so-called "black hat" hacking for so long that he did not have any helpful connections.

In comments throwing out the statutory challenges, Stadtmueller generally favors the prosecution

That said, in his language rejecting Hutchins' attempt to throw out his indictment charge by charge, Stadtmueller significantly sides with the prosecution, as follows:

Counts One and Seven: Whether the malware in question damaged computers

Stadtmueller argues the requisite details are there for the CFAA damage charges, but suggests the government may not be able to prove their case.

> These terms are sufficient to allege intent to cause damage. The burden will be on the government to prove this at trial.

Counts One Through Six: Whether software counts as a device

Perhaps Stadtmueller's most troubling ruling is that the wiretapping charges were sound (I say that because some very smart lawyers had suggested this was problematic from the start). He argues that the Seventh Circuit precedent doesn't cite case law and a bunch of cases (from other circuits) do.

> The majority of courts to consider this issue have entertained the notion that software may be considered a device for the purposes of the Wiretap Act. See Luis v. Zang, 833 F.3d 619, 630 (6th Cir. 2016) (accepting that a software could be a "device" for the purpose of the Wiretap Act); In re Carrier IQ, Inc., 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015) (concluding that a software was an "electronic, mechanical or other device"); Klumb v. Goan, 884 F. Supp. 2d 644, 661–62 (E.D. Ten. 2012) (analyzing spyware software as a device under Wiretap Act); Rene v. G.F. Fishers, Inc., 817 F. Supp. 2d 1090, 1094 (S.D. Ind. 2011) (holding that keystrokes are not electronic communications for the purpose of the Wiretap Act, but

> accepting the notion that software could be a device); Shefts v. Petrakis, 2012 WL 4049484, at *8–9 (C.D. Ill. 2012) (analyzing software as a device under the Wiretap Act); see also United States v. Barrington, 648 F.3d 1178, 1203 (11th Cir. 2011) (accepting that a keylogger software could be considered a scanning receiver, or a device, under 18 U.S.C. § 1029(e)(8)).
>
> The Court is in accord with the majority of courts to consider this issue. The Court also agrees with the government's position that Section 2510(5)'s reference to "mechanism," which is commonly defined as a "process, technique, or system for achieving a result" seems to encompass software. Mechanism, Merriam-Webster Dictionary, https://www.merriamwebster.com/dictionary/mechanism (accessed Jan. 22, 2019); see also United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (acknowledging that general technology statute should be read broadly in order to accommodate new developments).

Counts One, Four Through Eight, and Ten: Whether malware researcher MalwareTech intended to hack and wiretap

There are a bunch of problems with the way prosecutors claim Hutchins intended to do something it's not clear he did. To this complaint, Stadtmueller basically punts to trial, without hinting how he feels about the issue.

> These are arguments that go to the merits of the case, i.e., whether Hutchins had the requisite intent to commit the crimes charged.

Counts Two and Three: Whether you can charge wiretapping left and right

In its superseding indictment, the government tried to cover itself by charging both of two advertising related wiretapping charges. Hutchins challenged this, arguing they were trying to do the same thing (they are, practically). Stadtmueller ruled they weren't, legally.

> Each count contains an element required to prove the offense that is not required in the other count, and the counts require proof of different facts. There is no multiplicity.

Count Seven: Whether aid and abet without intent counts

This challenge is another intent based one, arguing that you can't aid and abet a crime that you didn't intend to accomplish in the first place. Stadtmueller seems skeptical but finds it passes this level of muster.

> Hutchins argues that he cannot be charged with attempt to aid and abet an attempt to violate the CFAA because Count Seven is pled "without reference to the intentional causing of damage," as stated in the statute. (Docket #92 at 5). The superseding indictment alleges that Hutchins attempted to cause damage, which encompasses the intent element. Whether the government can actually prove this at trial is a question for another time.

Counts Two and Three:

Whether Hutchins can be charged in the UK for a YouTube

Stadtmueller dismisses Hutchins' extraterritoriality challenge by saying that the government has at least alleged facts that meet this bar. In some of these details he gets the facts wrong, such as when he says that Hutchins himself pushed Kronos on YouTube.

> It also alleges that Hutchens used a YouTube video to promote the sale of Kronos, and referred interested purchasers of Kronos to Individual A.

This YouTube ploy by prosecutors was a key complaint by Hutchins' lawyers. Nevertheless, Stadtmueller rules that the government has at least alleged activities in EDWI.

> However, as stated, the charges sufficiently allege activity in the United States, specifically in the Eastern District of Wisconsin. There is no extraterritorial activity at issue.

That said, Stadtmueller lays this marker, disputing the government's view of extraterritoriality.

> However, because there is confusion about the proper standard to apply in the extraterritorial analysis, the Court takes this opportunity to clarify the issue in case it should arise in the future. There is a presumption against applying statutes extraterritorially because "Congress generally legislates with domestic concerns in mind." Small v. United States, 544 U.S. 385, 388 (2005) (quotations and citations omitted). This broad presumption applies in all cases, "preserving a stable background against which Congress can

> legislate with predictable effects." Morrison v. Nat'l Australian
>
> Therefore, the proper rule to apply is that of RJR Nabisco: if Congress has not evinced an affirmative intent to apply the statute extraterritorially, the Court must assess the focus of the statute, and determine whether the conduct relevant to the focus occurred in the United States. Under RJR Nabisco, some conduct could occur outside of the United States as long as the conduct relevant to the focus of the statute occurred inside the United States. However, as stated above, the conduct that the superseding indictment alleges took place in the United States. Therefore, the Court need not evaluate Sections 2512, 1343, or 1001 for extraterritorial application.
>
> For example, if, as it is alleged, Hutchins promoted his malware to individuals in the Eastern District of Wisconsin, then he could reasonably foresee being haled before this Court for trial on that issue.

Counts One Through Eight and Ten: Whether Hutchins can be charged in EDWI

Similarly, Stadtmueller dismisses another jurisdictional claim based on language that may get back to the intent issue.

> For example, if, as it is alleged, Hutchins promoted his malware to individuals in the Eastern District of Wisconsin, then he could reasonably foresee being haled before this Court for trial on that issue.

Count Nine: He's fucked on false statements until the other challenges work

This one, claiming that he can't be charged with false statements if he shouldn't be under FBI's jurisdiction in the first place, unsurprisingly fails so long as those Stadtmueller other charges.

> The Court finds that the FBI was properly within its jurisdiction to investigate these claims. Therefore, the charge that Hutchins lied to the FBI must also go forward.

It's hard to read what to take from all this. Stadtmueller clearly views some of these charges as flimsy. His views on the wiretap charge are the most surprising to me, and probably the most legally problematic for Hutchins (because of the advertising charges).

That said, Stadtmueller seems to have read this appropriately for what it is, the government effort to use any means available to punish Hutchins for being unable or unwilling to become the FBI's informant solely because he came to their attention for killing WannaCry.