Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Is The Hutchins Indictment Over Malware Unconstitutional?

By **Alex Berengaut**

Alex Berengaut

Law360, New York (August 17, 2017, 1:01 PM EDT) -- In May 2017, the "WannaCry" malware was used to launch a worldwide ransomware cyberattack. WannaCry encrypted files on victim computers and demanded a ransom payable in bitcoin to provide the encryption key. The attack was stopped when a British security researcher, Marcus Hutchins, accidentally discovered and activated a "kill switch" in the malware.

In a dramatic turn of events, Hutchins was arrested earlier this month by the FBI in Las Vegas as he was returning home from a cybersecurity conference. He wasn't charged for anything to do with WannaCry; rather, the government alleged that he had created and conspired to sell a different piece of malware, the "Kronos Banking trojan," a piece of software that recorded and stole user credentials and other personal identifying information. On Aug. 14, 2017, he pleaded not guilty to the charges against him.

Since Hutchins' indictment, commentators have questioned whether the creation and selling of malware — without actually using the malware — violates the two statutes under which Hutchins was charged: the Computer Fraud and Abuse Act and the Wiretap Act.[1] It is likely that these issues will be litigated as the case unfolds.

But there is another question raised by the indictment: whether it violates Hutchins' constitutional rights to charge him for his alleged conduct under any statute in this country. Several circuits — including the Seventh Circuit, where Hutchins' case will be heard — have recognized that the federal government cannot charge anyone, anywhere in the world irrespective of their connections to the United States.[2] As the Second Circuit has put it, "[i]n order to apply extraterritorially a federal criminal statute to a defendant consistently with due process, there must be a sufficient nexus between the defendant and the United States so that such application would not be arbitrary and fundamentally unfair."[3]

Case law on the sufficient nexus doctrine in the criminal context is scarce, and most cases involve terrorism or narcotics smuggling — situations where the nexus to the United States was clear. In analyzing the doctrine, accordingly, courts have looked to the equivalent due process protection in the civil context: the "minimum contacts" test for personal jurisdiction.[4] This test examines whether the

foreign defendant's conduct was directed at the United States such that it is appropriate to hale him or her into court in this country.

In this instance, the Hutchins indictment does not articulate a clear nexus between Hutchins and the United States. Hutchins is alleged to be a citizen and resident of the United Kingdom. He is accused of creating and conspiring to sell Kronos, a piece of malware that records and steals user credentials from "protected computers." The indictment defines "protected computer" to include a "computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States" — a definition broad enough to cover potentially every computer on the planet that is connected to the internet. Hutchins is not alleged to have created any part of Kronos in the United States, or for the purpose of affecting any particular U.S. person or interest inside or outside the country, or to have conspired to sell Kronos to anyone with those intentions.

Nor does the indictment allege a nexus to the United States based on the effects of Hutchins' foreign conduct. Courts have recognized that a sufficient nexus may exist if a defendant's foreign conduct causes certain types of effects in the United States. Yet while the indictment refers in conclusory terms to effects on interstate and foreign commerce, there are no factual allegations of specific losses caused by the Kronos malware inside the United States. Indeed, commentators have questioned whether there were any U.S. victims associated with the malware.[5]

Even if a U.S. victim could be identified and alleged in a superseding indictment, the government's theory appears to be that by creating Kronos, Hutchins aimed his wrongful conduct at the world financial system as a whole — including in the United States. If that is the theory, then it is in tension with long-standing principles of personal jurisdiction. In a seminal 1972 decision by Judge Henry Friendly, Leasco Data Processing Equipment v. Maxwell, the Second Circuit rejected the notion that a foreign defendant is subject to personal jurisdiction in the United States merely for directing his wrongful conduct at the world as a whole.[6]

In Leasco, the plaintiffs alleged that the defendants conspired to cause them to purchase stock in a British publisher at inflated prices.[7] One defendant was a British accounting firm, which allegedly certified the false financial statements upon which the plaintiffs relied.[8] The plaintiffs argued that personal jurisdiction existed over the defendant accounting firm because it "must have known that its reports on [the publisher] would be relied on by anyone interested in buying [the publisher's] shares."[9] The court disagreed, concluding that "[o]n that basis, accountants operating solely in London could be subjected to personal jurisdiction in any country whose citizen had purchased stock of a company they had audited."[10] While "such worldwide reliance may be, in a sense, foreseeable, it is not sufficiently so to constitute a basis of personal jurisdiction consonant with due process."[11]

An argument based on Leasco in the context of the Hutchins case is relatively straightforward. Insofar as the government might argue that it was foreseeable for Hutchins that Kronos would be used to cause harm in the United States, it was only foreseeable in the sense that Kronos would cause harm on a worldwide basis, including in the United States. And if that is the government's theory, then Hutchins could be "subjected to personal jurisdiction in any country" where Kronos was used. That is not enough, according to Leasco.

The government might also argue that the acts of Hutchins' unnamed co-conspirator should be attributed to him for purposes of the nexus analysis. As an initial matter, it is unclear if such attribution would change the nexus analysis for Hutchins; though the indictment alleges that the co-conspirator used an online video to demonstrate Kronos, sold Kronos on an online forum, and offered "crypting"

(services designed to conceal malware from anti-virus software) services for Kronos, it does not allege that the co-conspirator aimed his conduct at the United States, either. But even assuming that allegations could be included tying the co-conspirator to the United States, there is an argument that sufficient nexus—like personal jurisdiction—must be analyzed on an individual-by-individual basis. As the U.S. Supreme Court has put it: "Each defendant's contacts with the forum State must be assessed individually."[12]

It is also notable that Hutchins was arrested in the United States, which raises the question whether his presence in the United States at the time of his arrest is sufficient to establish a sufficient nexus for purposes of the Fifth Amendment. It may be challenging for the government to prevail on this argument, however, since defendants have been permitted to raise the sufficient nexus argument after trial (which, by definition, involves their physical presence in the United States),[13] and in one case, a court dismissed a multi-defendant indictment before trial, including for the defendant who was physically present in the United States.[14] The fact that these courts analyzed the nexus for the respective defendants by reference to their allegedly criminal acts — and not their physical presence in the United States at the time of trial — suggests that it is the allegations in the indictment (or the facts introduced at trial) that matter for purposes of nexus, not what happens later.

Lastly, it bears mentioning that sound policy arguments support the sufficient nexus doctrine. To be sure, as criminal conduct becomes increasingly transnational, it is important for U.S. law enforcement authorities to be able to prosecute extraterritorial conduct that harms U.S. persons or interests. This is particularly true in the context of cybercrime. But fundamental principles of fairness dictate that we only prosecute those who could reasonably expect to be prosecuted here. There is also the risk of reciprocity: If the United States does not enforce limitations on our ability to prosecute foreign citizens for extraterritorial conduct, why should other countries?

It remains to be seen whether the sufficient nexus doctrine will have a role to play in the Hutchins case. In the meantime, the indictment against Hutchins serves as a useful illustration of the doctrine and a reminder of its continuing relevance.

Alex Berengaut is a partner in the Washington, D.C., office of Covington & Burling LLP.

[1] Orin Kerr, The Kronos indictment: Is it a crime to create and sell malware?, Washington Post (Aug. 3, 2017) https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/08/03/the-kronos-indictment-it-a-crime-to-create-and-sell-malware

[2] In re Hijazi, 589 F.3d 401, 412 (7th Cir. 2009).

[3] United States v. Al Kassar, 660 F.3d 108, 118 (2d Cir. 2011).

[4] United States v. Klimavicius-Viloria, 144 F.3d 1249, 1257 (9th Cir. 1998).

[5] Thomas Fox-Brewster, Kronos Malware 'Dealer' on WannaCry Killer Charges: What Charges?, Forbes (Aug. 6, 2017), https://www.forbes.com/sites/thomasbrewster/2017/08/06/marcus-hutchins-case-

kronos-malware-not-hot-in-cybercrime/#3f1f6e006893

[6] 468 F.2d 1326 (2d Cir. 1972).

[7] Id. at 1330.

[8] Id.at 1331-32.

[9] Id. at 1342.

[10] Id.

[11] Id.

[12] Calder v. Jones, 465 U.S. 783, 790 (1984).

[13] United States v. Perlaza, 439 F.3d 1149, 1156 (9th Cir. 2006).

[14] United States v. Sidorenko, No. 14-CR-00341, Dkts. 11, 12, 54 (N.D. Cal. 2015) (dismissing the indictment including as to the defendant, Mauricio Siciliano, who was in custody).
