UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124

v.

MARCUS HUTCHINS,

Defendant.

DEFENDANT'S MOTION TO DISMISS THE INDICTMENT (IMPROPER EXTRATERRITORIAL APPLICATION OF LAW AND VENUE)

Defendant Marcus Hutchins seeks dismissal of all counts in the indictment because the extraterritorial application of United States law is improper in this case. Venue in the Eastern District of Wisconsin is also improper.

This Court should find that extraterritorial application of the law here is improper for two reasons. First, Congress has not clearly indicated that the Wiretap Act is intended to have extraterritorial reach, nor are the offenses, as they are charged, domestic. Second, the prosecution violates Mr. Hutchins' due process rights as to all counts because he had no substantial nexus with the United States during the relevant time period covered by the indictment.

Further, venue is improper for all counts because the indictment fails to establish that this District is the *locus delicti* of any element of the charged crimes,

nor that any effect was intended in this District. Accordingly, the Court should grant this motion and dismiss the indictment in its entirety.

***

The defense has concurrently filed two other separate motions to dismiss. The first seeks dismissal of all counts of the indictment under Federal Rule of Criminal Procedure 12(b)(3)(B)(v) for failure to state offenses. The second seeks dismissal of Counts Two and Six because they mis-describe the mental state required by the statutes at issue. This motion focuses on the improper extraterritorial application of law and venue.

BACKGROUND

Mr. Hutchins was arrested on August 2, 2017 on the pending indictment. At all times material to the allegations, he was a citizen and resident of the United Kingdom. (Indictment ¶ 1(b) (Dkt. No. 6).)

The six-count indictment centers around various alleged violations of the Computer Fraud and Abuse Act and the Wiretap Act. In Count One, Mr. Hutchins and his co-defendant are charged with conspiring to violate the CFAA. Counts Two through Four charge the defendants with advertising, sending, and selling an electronic communication interception device in violation of the Wiretap Act. Count Five charges that the defendants endeavored to intercept and procured another person to intercept electronic communications in violation

of the Wiretap Act. Finally, Count Six alleges that the defendants attempted to cause damage to a computer without authorization in violation of the CFAA.

As part of the purported conspiracy, the indictment alleges that Mr. Hutchins created the Kronos software, described as "a particular type of malware that recorded and exfiltrated user credentials and personal identifying information from protected computers." (*Id.* ¶¶ 3(e), 4(a).) It also alleges that Mr. Hutchins and his co-defendant later updated Kronos. (*Id.* ¶ 4(d).)

All other alleged overt acts in furtherance of the purported conspiracy pertain solely to Mr. Hutchins' co-defendant. Per the indictment, the co-defendant (1) used a video posted to YouTube to demonstrate how Kronos worked, (2) advertised Kronos on internet forums, (3) sold a version of Kronos, and (4) offered crypting services for Kronos. (*Id.* ¶¶ 4(b), (c), (e), (f), (g).)

Aside from a bare allegation that each offense was committed "in the state and Eastern District of Wisconsin and elsewhere," the indictment does not describe any connection to this District.

LEGAL STANDARD

The United States must have territorial jurisdiction over a defendant to pursue or hear a case against that person. The Seventh Circuit characterizes this requirement as a matter of whether a statute reaches outside the United States to conduct performed abroad. *Domanus v. Locke Lord LLP*, 847 F.3d 469, 482 (7th Cir. 2017); *In re Hijazi*, 589 F.3d 401, 408 (7th Cir. 2009). Other courts have treated this

requirement a question of subject-matter jurisdiction. *United States v. Al Kassar*, 660 F.3d 108, 118-19 (2d Cir. 2011).

A court must dismiss the indictment when it fails to state an offense. Fed. R. Crim. P. 12(b)(3)(B)(v); *United States v. Risk*, 843 F.2d 1059, 1060 (7th Cir. 1988). Furthermore, a defendant may move to dismiss a criminal case on the ground that the court lacks jurisdiction at any time during the pendency of the matter. Fed. R. Crim. P. 12(b)(2). Finally, the government is required to prosecute an offense in a district where it was committed. Fed. R. Crim. P. 18.

ARGUMENT

The United States government may not prosecute anyone anywhere in the world under federal criminal law. *Hijazi*, 589 F.3d at 412. The indictment should be dismissed because this case is an improper attempt to enforce United States law against Mr. Hutchins, who was a citizen and resident of the United Kingdom acting entirely abroad at all times material to the indictment. Furthermore, venue is improper because the *locus delicti* was not in this District.

1. **The Court Should Dismiss Counts Two Through Five Because Congress Did Not Intend the Wiretap Act to Have Extraterritorial Application and the Offenses are Not Domestic as Charged**

A fundamental premise of the American legal system is that "United States law governs domestically but does not rule the world." *Microsoft Corp. v. AT & T Corp.*, 550 U.S. 437, 454 (2007). As such, courts presume that statutes do not apply extraterritorially unless Congress says otherwise: "[a]bsent clearly

expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco, Inc. v. European Community*, --- U.S. ---, 136 S. Ct. 2090, 2100 (2016); *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 255 (2010); *see also Hijazi*, 589 F.3d at 409. United States criminal law generally does not reach acts committed by foreign nationals acting abroad against foreign interests due to the presumption against extraterritorial effect: "[w]hen a statute gives no clear indication of an extraterritorial application, it has none." *Morrison,* 561 U.S. at 255.

Courts have sometimes found that the presumption against extraterritoriality does not apply to criminal statutes, relying on nearly century-old precedent in *United States v. Bowman*, 260 U.S. 94 (1922). *See*, *i.e.*, *Al Kassar*, 660 F.3d at 118. In 2010, however, the Supreme Court made clear that the presumption applies "in *all* cases." *Morrison,* 561 U.S. at 261 (emphasis added); *see also United States v. Vilar*, 729 F.3d 62, 72 (2d Cir. 2013)

The Supreme Court has adopted a two-part analysis to determine whether a statute applies to foreign conduct. The court first asks whether "the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco*, 136 S. Ct. at 2101. If Congress does not clearly indicate that a statute is meant to apply extraterritorially, the court then determines whether the case involves a domestic application of the statute by looking to the "focus" of congressional concern. *RJR Nabisco*, 136 S. Ct. at 2101; *Morrison*, 561 U.S. at 249.

"If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad[.]" *RJR Nabisco*, 136 S. Ct. at 2101. But if the conduct relevant to the statute's focus occurred in a foreign country, "then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Id.*; *see also Kiobel v. Royal Dutch Petroleum*, 569 U.S. 108, 124-25 (2013).

There is evidence that Congress intended the CFAA—the legal basis of Counts One and Six—to have extraterritorial application. The CFAA prohibits certain conduct with respect to "protected computers," 18 U.S.C. § 1030(e)(2)(B), and the legislative history shows that Congress crafted the definition of that term with foreign-based attackers in mind. S. Rep. 104-357, at 4-5 (1996).

The Wiretap Act—at issue in Counts Two through Five—is different, though. That law does not reflect a clear congressional mandate that it should apply extraterritorially. Accordingly, courts have repeatedly found that it "has no extraterritorial force." *Huff v. Spaw*, 794 F.3d 543, 547 (6th Cir. 2015) (quoting *United States v. Peterson*, 812 F.2d 486, 492 (9th Cir. 1987)).

Section 2512 contains references to sending or transporting devices in "foreign commerce." But the Supreme Court has found that "general" or "fleeting" references to foreign commerce in a statute do not overcome the presumption against extraterritoriality. *Morrison*, 561 U.S. at 262-63; *see also*

EEOC v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) (*Aramco*). The legislative history does not show that Congress intended § 2512 to reach offenses in which the essential conduct elements are performed abroad.

Even assuming that the phrase "foreign commerce" alone in § 2512 is enough to overcome the presumption against extraterritoriality, that term is absent in § 2511. This omission shows at a minimum that Congress did not intend for § 2511 to have extraterritorial reach: "when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms." *Morrison*, 561 U.S. at 265. And Congress has explicitly stated that the Wiretap Act "regulates only those interceptions conducted within the territorial United States." S. Rep. 99-541, at 12 (1986). Thus, Congress did not intend for the Wiretap Act to have extraterritorial application.

This result raises the second prong of the extraterritoriality analysis: whether the indictment alleges a domestic application of the Wiretap Act. Counts Two, Three, and Four each rest on the claim that the defendants advertised, sent, and sold a device primarily useful for surreptitious interception in violation of 18 U.S.C. §§ 2512(a), (b) & (c)(i). The conduct that is the "focus" of congressional concern is the *advertising*, *sending*, and *selling* of such a device. Mr. Hutchins' alleged actions were performed abroad, in the countries in which he

was located. And on the face of the indictment, no specific act or result is alleged to have occurred within the United States.

As for Count Five, Mr. Hutchins and his co-defendant allegedly endeavored to intercept and procured someone else to intercept electronic communications in violation 18 U.S.C. § 2511(a). Congress' concern here—the *actus reus*—focused on *endeavoring* and *procuring* another person to perform an interception. Mr. Hutchins' conduct, as it is alleged in the indictment, occurred abroad. And no specific act or result is alleged by the indictment to have occurred in United States.

In sum, Counts Two through Five should be dismissed because they impermissibly attempt to apply United States law to foreign conduct. The presumption against extraterritoriality should defeat those counts.

2. The Court Should Dismiss All Counts Because Their Extraterritorial Application Violates Mr. Hutchins' Constitutional Right to Due Process

The Fifth Amendment requires a "sufficient nexus" between the United States and a foreign national facing criminal prosecution to ensure that application of this country's law "would not be arbitrary or fundamentally unfair." *United States v. Davis,* 905 F.2d 245, 248–49 (9th Cir. 1990); s*ee also Hijazi*, 589 F.3d at 401 (Lebanese citizen living in Kuwait properly raised due process objections to his indictment).

This requirement, which is akin to the "minimum contacts" test for personal jurisdiction in the civil context, "ensures that a United States court will assert jurisdiction only over a defendant who should reasonably anticipate being haled into court in this country." *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1257 (9th Cir. 1998) (internal quotation marks omitted). Even when Congress clearly shows that it intends a criminal statute to apply extraterritorially, the law may only do so if it doesn't violate the Fifth Amendment. *Al Kassar*, 660 F.3d at 117; *United States v. Yousef,* 327 F.3d 56, 86 (2d Cir. 2003).

Mr. Hutchins' prosecution in the United States is arbitrary and fundamentally unfair. The indictment does not articulate a clear nexus between Mr. Hutchins and the United States. During the time period covered by the indictment, he was a foreign citizen and resident. He is not alleged to have created or updated Kronos in the United States. He is not alleged to have developed Kronos for the purpose of affecting any interest inside the country, or to have conspired or attempted to sell Kronos to anyone with that intention.

Nor does the indictment allege a sufficient nexus to the United States based on the *effects* of Mr. Hutchins' foreign conduct. As an initial matter, a jurisdictional nexus exists for non-citizens acting entirely abroad only if "the aim of their activity is to cause harm inside the United States or to U.S. citizens or interests." *Al Kassar*, 660 F.3d at 117; *see also Klimavicius-Viloria,* 144 F.3d 1257

(sufficient nexus exists when "an attempted transaction is aimed at causing criminal acts within the United States"). In other words, "jurisdictional nexus is determined by the *aims* of the conspiracy, not by its *effects*." *Al Kassar*, 660 F.3d at 119 (emphasis added).

That said, the indictment alleges no particular domestic effect of Mr. Hutchins' foreign conduct. It refers in conclusory terms to effects on interstate and foreign commerce, but it makes no factual allegations of specific damage or consequence caused by Kronos inside the United States. A foreign defendant like Mr. Hutchins is not subject to the jurisdiction of the United States merely for directing conduct toward the world at large—it must be foreseeable that the conduct could cause harm specifically in the United States. *See Leasco Data Processing Equipment v. Maxwell*, 468 F.2d 1326, 1330, 1342 (2d Cir. 1972).

To the extent that it was foreseeable that Kronos might be used to cause harm in the United States, it was only foreseeable in the sense that Kronos could cause harm anywhere in the world—including in the United States. If that conduct alone constitutes a sufficient nexus to hale Mr. Hutchins into a U.S. court, he could theoretically be haled into any court in the world. Subjecting foreign defendants to such an expansive theory of jurisdiction is arbitrary and fundamentally unfair.

Finally, the alleged acts of Mr. Hutchins' co-defendant do not serve as a proxy to create a sufficient nexus for Mr. Hutchins. First, the indictment does not

establish that the co-defendant had any nexus to the United States. And though the indictment alleges that the co-defendant used an online video to demonstrate Kronos, advertised Kronos in online forums, sold Kronos, and offered "crypting" services for Kronos, it does not allege that the co-conspirator directed any of this conduct at the United States or caused any effect in the United States.

Second, even assuming the co-defendant has a sufficient nexus to the United States, that person's alleged acts cannot be attributed to Mr. Hutchins for purposes of establishing Mr. Hutchins' nexus. The Court must find an independent sufficient nexus for each individual: "Each defendant's contacts with the forum State must be assessed individually." *Calder v. Jones*, 465 U.S. 783, 790 (1984). For all these reasons, the indictment should be dismissed.

3. Dismissal is Warranted Because Venue in the Eastern District of Wisconsin is Improper

The Constitution guarantees that "[t]rial of all crimes . . . shall be held in the State where the said crimes shall have been committed." U.S. CONST. Art. III, § 2, cl. 3. Further, the Sixth Amendment provides an accused the right "to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." Venue protections "touch closely the fair administration of criminal justice and public confidence in it." *United States v. Johnson*, 323 U.S. 273, 276 (1944). It is not a "mere technicality," particularly for

"computer crimes in the era of mass connectivity." *United States v. Auernheimer*, 748 F.3d 525, 529 (3d Cir. 2014).

Venue must be proper for each count of the indictment. *United States v. Tingle*, 183 F.3d 719, 726 (7th Cir. 1999). Unless a statute explicitly provides otherwise, venue is proper in any district where an offense was begun, continued, or completed. 18 U.S.C. § 3237(a); *United States v. Sidener*, 876 F.2d 1334, 1337 (7th Cir. 1989). Venue is only proper if a defendant was physically present in the district when they committed unlawful acts, or in a district where the acts were "intended to have an effect." *United States v. Muhammad*, 502 F.3d 646, 655 (7th Cir. 2007).

If Congress does not specify where a crime should be deemed to have occurred, the "*locus delicti* must be determined from the nature of the crime alleged and the location of the act or acts constituting it." *United States v. Cabrales*, 524 U.S. 1, 6-7 (1998); *Tingle,* 183 F.3d at 726. To determine the *locus delicti*, a court looks to the key verbs in the statute to identify the criminal acts that constitute the offense. *Tingle,* 183 F.3d at 726.

Count One is a charge of conspiracy to violate 18 U.S.C. § 1030(a)(5)(A). Count Six alleges that Mr. Hutchins and his co-defendant attempted to violate the same law. Section 1030(a)(5)(A) makes it illegal to "knowingly *cause[] the transmission* of a program, information, code, or command, and as a result of such conduct, intentionally *cause[] damage* without authorization, to a protected

computer." (Emphasis added). This language indicates that the crucial elements of the crime occur where the defendant causes the transmission and where damage is caused.

Here, the indictment reflects that Mr. Hutchins was on foreign soil, and any acts he performed occurred there. There is no indication that damage was caused in the Eastern District of Wisconsin—or, indeed, that any damage occurred at all. At best, a buyer was present in this District. But the buyer would then need to use Kronos to cause damage in the District for venue to lie. Nothing in the indictment supports that conclusion.

Venue is also improper for the counts brought under the Wiretap Act. Counts Two, Three, and Four charge violations of 18 U.S.C. § 2512. In relevant part, that section makes it illegal to *send*, *sell*, or *disseminate an advertisement* of an electronic device that is primarily useful for surreptitious interception of communications. 18 U.S.C. §§ 2512(a), (b) & (c)(i). But Mr. Hutchins' purported acts to send, sell, or advertise were performed in a foreign country. And the indictment does not reflect any connection to, or effect intended in, the Eastern District of Wisconsin.

Count Five charges that the defendants endeavored to intercept and procured someone else to intercept an electronic communication in violation of 18 U.S.C. § 2511(a). That section prohibits *intercepting*, *endeavoring* to intercept, or *procuring* another person to intercept any wire, oral, or electronic

communication. But again, Mr. Hutchins' alleged acts occurred abroad, and there is no indication that any act was performed or any effect was intended in this District. Thus, venue in the Eastern District of Wisconsin is improper for all counts.

CONCLUSION

For the foregoing reasons, this Court should dismiss the indictment.

DATED: March 30, 2018

Respectfully submitted,

/s/ Marcia Hofmann
MARCIA HOFMANN
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Email: marcia@zeitgeist.law
Telephone: (415) 830-6664

/s/ Brian E. Klein
BRIAN E. KLEIN
Baker Marquart LLP
2029 Century Park E – Suite 1600
Los Angeles, CA 90067
Email: bklein@bakermarquart.com
Telephone: (424) 652-7800

/s/ Daniel W. Stiller
DANIEL W. STILLER
DStillerLLC
Box 511130
Milwaukee, WI 53203
Email: dan@dstillerllc.com
Telephone: (414) 207-3190

Attorneys for Marcus Hutchins