UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**Crim. No. 21-cr-00032 (DLF)**
	:	
v.	:	
	:	
GUY WESLEY REFFITT,	:	
	:	
Defendant.	:	

MOTION TO COMPEL DEFENDANT TO PRODUCE EVIDENCE IN UNENCRYPTED STATE

The government respectfully moves for an order compelling the defendant to produce a critical piece of evidence – his Microsoft Surface Pro laptop computer – in an unencrypted state. The government proposes a two-step process: First, the defendant should be ordered to place his face in front of the computer's camera, so that the computer can be biometrically unlocked. Second, if the biometric attempt does not unlock the computer, the defendant should be ordered to type his passcode or PIN into the computer.

I. Background[1]

A. The defendant's crimes

The government has evidence that the defendant travelled from his home in Wylie, Texas, to Washington, D.C., with an AR-15 rifle and a Smith & Wesson .40 caliber handgun, to participate in the riot and obstruction of Congress that occurred at the U.S. Capitol on January 6, 2021. While at the Capitol, the defendant, armed with his handgun in a holster on his waist, confronted U.S. Capitol Police officers on the west side stairs, just north of the temporary scaffolding. The defendant charged at the officers, who unsuccessfully tried to repel him with two different types

[1] The government is proceeding here via proffer. If the Court deems it necessary, the government can provide evidence, either by declaration or by live testimony at the hearing scheduled for July 14.

of less-than-lethal projectiles before successfully halting his advances with pepper spray.

On January 11, 2021, the defendant threated his children if they reported him to law enforcement for his crimes on January 6.

On June 16, 2021, the grand jury returned a superseding indictment, charging the defendant with five felony counts: 18 U.S.C. § 231(a)(2) – Civil Disorder (Transportation); 18 U.S.C. §§ 1512(c)(2), 2 – Obstruction of Official Proceeding and Aiding and Abetting; 18 U.S.C. § 1752(a)(1) and (b)(1)(A) – Restricted Building or Grounds While Armed; 18 U.S.C. § 231(a)(3) – Civil Disorder (Interference); and 18 U.S.C. § 1512(a)(2)(C) (Obstruction of Justice – Hindering Communication Through Physical Force or Threat of Physical Force).

B. <u>The defendant's arrest and the recovery of electronic evidence</u>

On January 16, 2021, the FBI arrested the defendant and executed a search warrant (4:21-mj-036 (E.D. Tex.)) on his house in Wylie, Texas.[2] The FBI recovered the following 21 digital devices:

- Cell phones and tablets:
    - Item 1B4: Black Apple iPhone in a blue, gray and clear colored "Raptic Shield" case located on the defendant's person.
    - Item 1B15: Black Apple iPhone with no visible model number or other markings, in gray and clear Pelican case, located in a white Chevrolet Colorado pick-up truck, specifically inside the storage shelf of the center console, forward of the gear shift lever.

[2] The FBI contemporaneously executed search warrants on the defendants' two vehicles, in 4:21-mj-34 and -35 (E.D. Tex.).

- Item 1B16: Black Apple iPhone, model A1778, in black and clear Pelican case, located in master bedroom closet.
- Item 1B5: Silver Apple iPad Model A1550; FCC ID: BCGA1550; s/n DLXRD2RZGHMK, located inside gun safe.

- Computers:
  - Item 1B17: Silver and black HP Pavilion DM3 laptop computer, model DM3-1039WM, S/N CNC94139YY, with "American Sniper, One Shot one kill" sticker on the outside and U.S. Confederate battle flag and U.S. American flag stickers near keyboard, located on the fifth shelf of a built-in shelving unit to the right of the gun safe in the master bedroom closet.
  - Item 1B11: Silver Apple MacBook Air, model A1465, S/N C02NF2EHG083, located on the fifth shelf of a built-in shelving unit to the right of the gun safe in the master bedroom closet.
  - Item 1B12: Silver Apple MacBook Air, model A1466, S/N C17N3716G085, located on the fifth shelf of a built-in shelving unit to the right of the gun safe in the master bedroom closet.
  - Item 1B20:[3] Silver Microsoft Surface Pro tablet computer with black detachable keyboard, model 1796, 128GB, S/N 014952773253, located on top of coffee table in living room.
- Storage media:

[3] Item 1B20 is listed twice, as it includes both the computer itself and an external hard drive.

- Item 1B8: Black Seagate "FreeAgent Goflex" 1TB external hard drive, s/n NA05L6ER, located inside gun safe in the master bedroom closet.
- Item 1B9 (all located inside gun safe in the master bedroom closet):
  - Red SanDisk 4GB memory card;
  - Two Max Flash 4GB memory cards;
  - Kingston Micro SD Adapter;
  - White TP Link 300 MBPS "TL-WN821N" thumbdrive;
  - Cruzer Glide 32GB thumbdrive;
  - Silver Verbatim 32GB thumbdrive with both USB and iPhone connection;
  - Black SanDisk "Connect Wireless Stick" thumbdrive
- Item 1B18 (located inside black messenger-style bag in living room):
  - Red and black SanDisk Cruzer Blade 16GB thumbdrive;
  - black SanDisk adapter for Micro SD card
- Item 1B20: Seagate "Expansion Portable Drive" external hard drive, S/N NA8ZTJG8, located on top of coffee table in living room.

- Camera:
  - Item 1B22: Grey fabric bag containing white Kodak Pixpro Orbit360 4K camera, S/N M054009013, located on top of coffee table in living room.

The FBI sent the devices to Washington, D.C., to be processed. On February 26, 2021, Magistrate Judge Meriweather approved a warrant (21-sw-55) to search these devices.[4]

[4] The government had obtained a nearly identical warrant two weeks earlier (21-sw-41), but the

The instant motion concerns Item 1B20 (the Microsoft Surface Pro tablet computer) and Item 1B22 (the Kodak Pixpro Orbit360 4K camera). For the remaining devices, the FBI either accessed and processed them pursuant to the warrant (and the government produced the extractions to the defense in discovery), or the FBI determined that they were damaged and/or did not hold any relevant data.

Item 1B20 (the Microsoft Surface Pro tablet computer) will hereinafter be referred to as the "Subject Device."

C. The basis for the government's assertion that relevant evidence is on the Subject Device.

While at the Capitol on January 6, the defendant was wearing on his head a black tactical helmet with an attached video camera, pictured below:

devices were not processed before the warrant expired.

During the search warrant at the defendant's home, the FBI recovered both the helmet and the camera. The helmet was in a bag in the defendant's car. This is a photo:

The camera, a Kodak Pixpro Orbit360 4K – which is similar in style to a "Go Pro" – was in a cloth bag on top of a table in the living room. This is the same location in which the FBI recovered the Subject Device.

At the time of his arrest on January 16, 2021, Reffitt, after being *Mirandized*, stated that while at the Capitol he was wearing a black bump helmet with a Kodak Orbital 360 4k attached. Reffitt said that the camera was similar to a Go Pro. When asked if he was recording while at the Capitol, Reffitt said, "I was recording the events at the Ellipse, less than one second at the Capitol. Didn't record anything."

One of Reffitt's family members, who will be referred to as CW-1, reported to the government that the Subject Device is Reffitt's primary computer.[5] CW-1 stated that, after Reffitt returned home from the Capitol riot, Reffitt used the Subject Device to show the family videos from January 6 that he said he had recorded on his helmet-mounted camera; CW-1 said that the defendant apparently had copied these videos onto the Subject Device, and then used the Subject Device to show the videos to the family. Indeed, CW-1 surreptitiously recorded the defendant's voice as the defendant narrated some of the videos shown on the Subject Device for the family.

In one of those surreptitious recordings, from January 9, 2021, the defendant states:

GUY REFFITT: I got a one-second video, but the camera fucking turned off where I started hitting it.

OTHER PERSON: You didn't take any photos?

[5] In his custodial interview, Reffitt stated that the Subject Device belonged to his wife:

AGENT: And normally where do you keep your computer, is it a laptop?

GUY REFFITT: Yes

AGENT: Where do you keep your laptop?

GUY REFFITT: It should be in the house somewhere.

AGENT: Just somewhere?

GUY REFFITT: My kids move stuff around quite often

AGENT: What kind of computer is it?

GUY REFFITT: It's my wife's computer, but it's a Microsoft Surface Pro.

GUY REFFITT: No, it's on Fox News. Close enough. I did. I took video. But I had to turn it off when because the battery was dying. But when I got to the Capitol and went to storm the Capitol and went up the stairs and was getting shot by bullets, rubber bullets <inaudible>. One second after I turned it on....

The government has not corroborated the defendant's statement, made both to his family and the FBI, that he only recorded for "one second" while at the Capitol. Indeed, the news video footage of the defendant at the Capitol shows the camera still attached to the helmet after the defendant's interference with the Capitol Police officers – though it is unclear from the news footage if the camera is still recording. Regardless, there are three reasons why the defendant's statements do not undermine the government's instant request:

First, the defendant may be mistaken or intentionally misleading about the extent of the video that his camera captured at the Capitol.

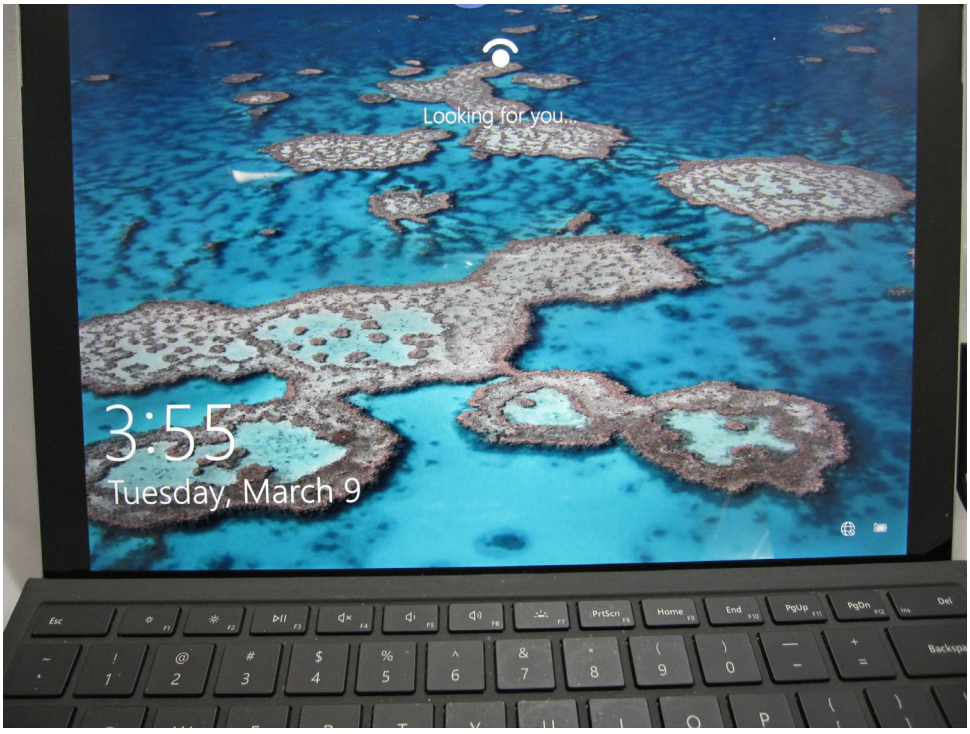
Second, even a short video clip may capture a relevant statement, item (such as the defendant's firearm), or interaction (such as the positioning of the defendant and/or the officers with whom he engaged during the riot).

Third, the defendant acknowledges recording earlier in the day at the Ellipse prior to moving to the Capitol, and those recordings may capture relevant statements (such as the defendant's professed intent) and items (such as the defendant's firearm).

An FBI forensic examiner reviewed the Kodak camera and determined that there were no intact – i.e., playable – video files on the SD card inside the camera. However, forensic examination of the SD card showed that three video files had been on the SD card but had been deleted on January 9, 2021. The file names and sizes were "DC 001.mp4" (4.3 GB); "DC 002.mp4" (2.3 GB), and "100_0003.mp4" (2.8 MB). Based on this information, as well as CW-1's statements, the government believes that at least these three videos files may have been transferred to the Subject Device.

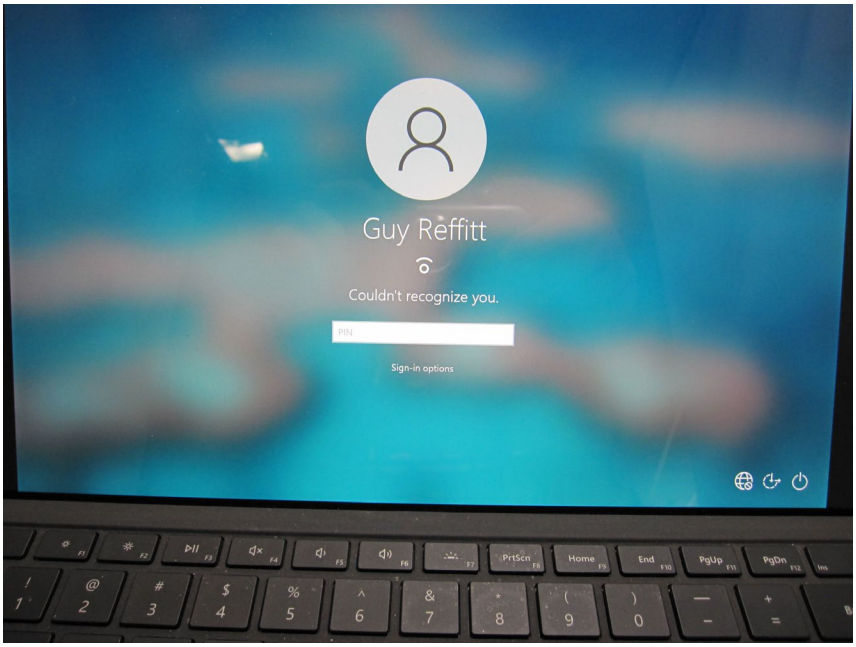
II. Forensic Examination of the Subject Device

When powered on, the Subject Device first has an option for a biometric unlock. The laptop's camera[6] looks for the face of the owner:

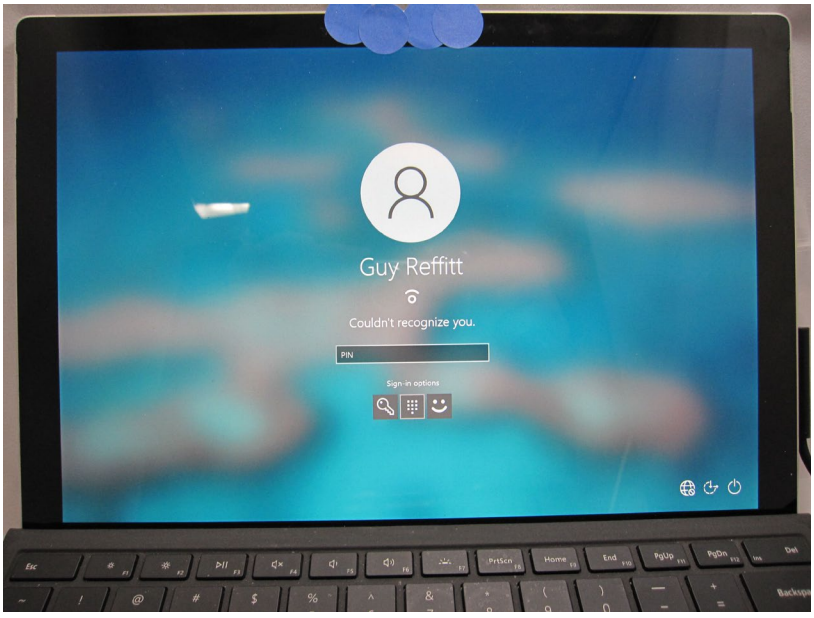


[6] The FBI's forensic examiner covered the camera with stickers, so the camera would not be accessible.

If the camera cannot locate the face of the owner, the system displays the name of the owner ("Guy Reffitt") and reports that it "couldn't recognize you":



The system asks the user to input a PIN. A user also may select "sign-in options," which displays three options for unlocking the computer: a key (PIN), a touchpad (passcode), and a smiley face (facial biometric).



The FBI attempted entry of certain likely PINs and passcodes, but none were successful. The FBI believes the system may freeze or delete if a certain number of incorrect PINs or passcodes are entered.

In an effort to access the Subject Device without seeking the Court's intervention, the government sought the defendant's consent to unlock the Subject Device. On June 3, 2021, defense counsel informed the government that the defendant would refuse to voluntarily provide the Subject Device in an unencrypted state – i.e., that the defendant would refuse to voluntarily submit his face (biometrics) to unlock the Subject Device, that the defendant would refuse to provide the government with his passcode for the Subject Device, and that the defendant would refuse to enter his passcode into the Subject Device to unlock it. At the status hearing on June 4, 2021, defense counsel confirmed these positions.

III. Argument

This Application seeks an order under the All Writs Act requiring the defendant to assist in the execution of the previously issued search warrant by producing the Subject Device in a fully unencrypted and unlocked state. This could be accomplished by making the Subject Device available at the jail or a government facility, where, first, the Subject Device could be placed in front of the defendant's face, so that it could be biometrically unlocked. Second, if the biometric unlock fails, the defendant could type the password or PIN on the Subject Device's keyboard without being observed by the government.

The requested relief would not violate the defendant's Fourth or Fifth Amendment rights. With respect to the Fourth Amendment, there is only minimal intrusion on the defendant's privacy, and there is probable cause that the defendant's face can unlock the Subject Device (and lead to

the recovery of relevant evidence). With respect to the Fifth Amendment, Reffitt's entering his password into the Subject Device does not violate his privilege against self-incrimination, because his act of production would not be testimonial, since the only potentially testimonial component implicit in his act of producing the unlocked/unencrypted device is a foregone conclusion.

A. The All Writs Act empowers this Court to order the requested relief.

The All Writs Act permits federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). It is "a residual source of authority to issue writs that are not otherwise covered by statute." *Penn. Bureau of Correction v. United States Marshals Serv.*, 474 U.S. 34, 43 (1985). The power conferred by the Act extends to anyone "in a position to frustrate the implementation of a court order or the proper administration of justice," as long as there are "appropriate circumstances" for doing so. *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Courts have authority under the All Writs Act to issue supplemental orders to facilitate the execution of search warrants. In *New York Telephone*, for example, the district court had issued an order authorizing federal agents to install pen registers in two telephones and directing the New York Telephone Company to furnish "all information, facilities and technical assistance" necessary to accomplish the installation. *Id.* at 161. The telephone company moved to vacate the order, arguing that neither Federal Rule of Criminal Procedure 41 nor the All Writs Act "provided any basis" for it. *Id.* at 163. The Supreme Court, however, held that the order was "clearly authorized by the All Writs Act" as a necessary and appropriate means of effectuating the installation of the pen registers. *Id.* at 172.

In a situation similar to the one at hand, the Third Circuit recently upheld an order under the All Writs Act requiring a defendant to produce unencrypted copies of electronic devices seized from his residence. In *United States v. Apple MacPro Computer*, 851 F.3d 238, 242 (3d Cir. 2017), officers had executed a search warrant at the defendant's home, seizing a computer and two encrypted external hard drives. A review of the computer revealed one image of child pornography, evidence that the computer had accessed child pornography websites, and logs showing that child pornography had been transferred to the external hard drives. *Id.* In addition, the defendant's sister told investigators that she had seen child pornography on the external hard drives. *Id.* at 242-43. When the defendant refused to provide the encryption passwords, the government moved for an order under the All Writs Act requiring him to produce the devices in a fully unencrypted state, which the magistrate judge issued. *Id.* at 243. On appeal, the Third Circuit upheld the order under the Act, holding that it "was a necessary and appropriate means of effectuating the original search warrant." *Id.* at 246. The court reasoned that, as in *New York Telephone*, the defendant was not far removed from the underlying controversy, compliance with the order required minimal effort, and without the defendant's assistance there was no conceivable way in which the search warrant could be effectuated. *Id.*

District courts have similarly issued orders under the All Writs Act compelling the owners of devices to assist with circumventing password protections or decryption where the device at issue was the subject of a valid search warrant or grand jury subpoena:

- A district judge in the Northern District of California issued an order compelling a defendant to produce three devices in an unencrypted state, once the government made an adequate showing that the defendant was the owner of the devices, that he

had the ability to decrypt them, and that the devices held relevant evidence (there, child pornography). *United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018), *aff'g Matter of Search of a Residence in Aptos, California 95003*, No. 17-MJ-70656-JSC-1, 2018 WL 1400401 (N.D. Cal. Mar. 20, 2018).

- A district judge in the District of Colorado granted an application under the All Writs Act to require the owner of a computer seized pursuant to a search warrant to produce it in an unencrypted state, after finding that the government has met its burden to show by a preponderance of the evidence that the computer belonged to the defendant and that the defendant could access the encrypted contents of the computer by entering a password. *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012).
- A district judge in the District of Vermont denied a motion to quash a grand jury subpoena requiring an individual to produce a laptop computer in unencrypted state, finding that the individual had no act-of-production privilege to refuse to comply, given that the government already knew of the existence and location of the files at issue. *In re Boucher*, No. 2:06-MJ-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009).

In accordance with these principles, this Court should issue an order under the All Writs Act requiring the defendant to assist with the execution of the search warrant by producing the Subject Device in a fully unlocked and unencrypted state. Without his assistance, the search warrant will be frustrated, because the government will be unable to search the Subject Device for

the information specified in the warrant. Defendant Reffitt is not far removed from the underlying controversy, and the requested relief will not impose an unreasonable burden on him; he need only enter the necessary password, without being observed by the government.

B. The requested relief comports with the Fourth Amendment.

Here, the government's two-step proposed process first includes an attempted biometric unlock – i.e., placing the Subject Device in front of the defendant's face, and allowing the Subject Device's camera to use the defendant's irises and/or facial features to unlock the device.

Magistrate Judge Meriweather, in the warrant issued in 21-sw-55, already found that there was probable cause to believe that evidence would be located on the Subject Device. The instant motion simply seeks the Court's assistance in unlocking the device so that the evidence can be accessed.

Magistrate Judge Harvey, in an opinion on the related topic of ex ante approval of compulsion of biometric features, held that the government may compel the use of an individual's biometric features on an electronic device during the execution of a search warrant "if, at time of the compulsion, the government has ([1]) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and ([2]) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is a user of the device." *Matter of Search of [Redacted] Washington, District of Columbia*, 317 F. Supp. 3d 523, 532-33 (D.D.C. 2018).[7] Judge Harvey cautioned that the government should "continue to seek prior authorization for the

[7] The opinion's first category, about conducting the biometric unlock expeditiously and while on the premises being searched, is not appliable here.

compelled use of an individual's biometric features to unlock digital devices even where the search of such devices is permitted by a warrant." The instant motion comports with that requirement.

On the first prong, there is reasonable suspicion – in fact, there is probable cause – that Reffitt has committed a criminal act that is the subject of the warrant. The grand jury has found probable cause to indict the defendant, and Judge Meriweather found probable cause that evidence of a crime would be located in the Subject Device.

On the second prong, there is reasonable suspicion that Reffitt's biometric features will unlock the Subject Device. Indeed, at the login screen, the device's camera is specifically looking for the face and/or irises of "Guy Reffitt" to authorize the unlock.

The requested relief therefore comports with the Fourth Amendment.

C. The requested relief would not violate the defendant's Fifth Amendment right against self-incrimination.

1. *A biometric unlock does not implicate the Fifth Amendment.*

An order compelling the defendant to place his face in front of a computer's camera would not run afoul of the defendant's Fifth Amendment right against self-incrimination. The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." A compelled communication, however, must be testimonial in order to receive Fifth Amendment protection. *See Fisher v. United States*, 425 U.S. 391, 409 (1976). The Supreme Court has held that in order to be considered testimonial, "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210 (1988). It is only under these circumstances that a person is unconstitutionally compelled to be a "witness" against himself. *Id.*

The Supreme Court has held that certain acts are not within the Fifth Amendment privilege against self-incrimination, even though the acts may be incriminating. *See, e.g., Schmerber v. California*, 384 U.S. 757, 765 (1966) (suspect may be compelled to furnish a blood sample); *Gilbert v. California*, 388 U.S. 263, 266-67 (1967) (suspect may be compelled to provide a handwriting exemplar); *United States v. Dionisio*, 410 U.S. 1, 7 (1973) (suspect may be compelled to provide a voice exemplar); *United States v. Wade*, 388 U.S. 218, 221-22 (1967) (suspect may be compelled to stand in a lineup); *Holt v. United States*, 218 U.S. 245, 252-53 (1910) (suspect may be compelled to wear particular clothing). Similarly, a biometric unlock is not testimonial and not within the defendant's Fifth Amendment privileges.

"[T]he seizure of any incriminating information found *on* the phones or computers discovered during the search of the premises would not violate the Fifth Amendment because the 'creation' of that information was voluntary and 'not compelled' within the meaning of the privilege against self-incrimination." *Matter of Search of [Redacted]*, 317 F. Supp. 3d at 534 (internal alterations and quotations omitted; emphasis in original).

2. *Ordering the defendant to decrypt the Subject Device – i.e., type his password onto the keyboard – does not run afoul of the Fifth Amendment*

The act of producing the Subject Device in an unencrypted and unlocked state does not implicate the Fifth Amendment, because The Fifth Amendment does not proscribe the compelled production of evidence if the facts communicated by the act are foregone conclusions.

This case is governed by the Supreme Court's decision in *Fisher*. There, the government had issued summonses for several categories of documents related to an individual's tax returns. 425 U.S. at 394-95. In concluding that enforcement of the summonses did not violate the Fifth

Amendment, the Supreme Court distinguished between two types of communications inherent in the production of the records. On the one hand, the Court held that the contents of the records were not privileged because the documents had been prepared voluntarily prior to the issuance of the summonses and were therefore not the taxpayer's compelled testimony. *Id.* at 409-10. On the other hand, the Court recognized that the act of production itself could communicate potentially incriminating facts, including, on that facts of that case, a tacit concession that the papers existed, that the respondent possessed them, and that they were authentic. *Id.* at 410. Nevertheless, the Court held that the compelled act of producing the papers did not implicate the Fifth Amendment because "[t]he existence and location of the papers [were] a foregone conclusion and the taxpayer add[ed] little or nothing to the sum total of the Government's information by conceding that he in fact ha[d] the papers." *Id.* at 411. In other words, because the potentially testimonial aspects of the act of production were a "foregone conclusion," compliance with the summonses became a question "not of testimony but of surrender." *Id.* (quoting *In re Harris*, 211 U.S. 274,279 (1911)).

The analysis set forth in *Fisher* is now known as the "foregone conclusion" doctrine. *See United States v. Ponds*, 454 F.3d 313, 319 (D.C. Cir. 2006). For the doctrine to apply, the government need only demonstrate with "reasonable particularity" its independent knowledge of the facts implicitly communicated by the act of production. *Id.* at 321 (quoting *United States v. United States v. Hubbell*, 167 F.3d 552, 579-80 (D.C. Cir.1999).

As in *Fisher* and *Ponds*, the act of producing an electronic device in an unencrypted state has potentially testimonial components similar, but not identical, to the potentially testimonial components involved in the act of responding to a subpoena for particular categories of documents. First, producing documents in response to a category-based subpoena demonstrates the

document's existence; producing an unencrypted device will similarly demonstrate the device's existence. Second, compliance with a category-based subpoena demonstrates possession and control over the documents; producing an unencrypted device will similarly demonstrate possession and control over the device.

However, there is an important distinction in the act-of-production privilege between a subpoena and an All Writs Act demand. The knowledge implicitly demonstrated by the act of producing documents in response to a subpoena differs significantly from producing an already-seized device in an unencrypted state. Producing papers in response to a category-based subpoena implicitly demonstrates knowledge of the contents of the papers produced: It demonstrates the "belief that the papers are those described in the subpoena." *Fisher*, 425 U.S. at 410. In contrast, producing a device in an unencrypted state implicitly demonstrates knowledge of the encryption password for the device, but it does not necessarily imply knowledge of the device's contents, because such knowledge is not needed to produce the device in an unencrypted state.

There is a further important distinction between this case and the child pornography cases in which the foregone conclusion doctrine often arises. In those cases, the files themselves were contraband, and thus the act of producing the device in an unencrypted state could support one of the elements the government must prove at trial: the defendant's knowledge of the presence of the illegal files on the device. But such concerns are not present here, because there is no allegation that the files on the Subject Device are themselves contraband. In other words, while the government could plausibly argue that a defendant's unlocking of a computer that contained child pornography demonstrated that defendant's knowledge of the contents of the files on the computer, here Reffitt's unlocking of the Subject Device is irrelevant to his knowledge of the

contents on the device. Simply, the files on the Subject Device are relevant evidence *even if* Reffitt did not know of their existence or contents. The fact that the relevance of the evidence sought from the Subject Device does not turn on Reffitt's knowledge of whether these files are stored on the device further negates any Fifth Amendment implications of the government's motion.

All of the potentially testimonial assertions implicit in Reffitt's act of producing the decrypted Subject Device are already known to the government. The government knows that the Subject Device exists, that Reffitt had ownership or control over it, that Reffitt can decrypt it, and that it contains relevant video files. Under the foregone conclusion doctrine, Reffitt's act of producing the decrypted Subject Device is not protected by the Fifth Amendment.

First, there is no question that the Subject Device exists. The FBI located it in Reffitt's living room, and it is now in the FBI's possession.

Second, there is no question that Reffitt had ownership or control over the Subject Device. It welcomes him by name at the login screen, CW-1 stated that Reffitt often used the device, and he admitted that it was his device during his custodial interview.

Third, and similarly, because Reffitt's name is on the login screen, and because he was often seen using the Subject Device, the government knows that Reffitt can unlock or decrypt the Subject Device.

Fourth, the government knows the Subject Device contains relevant video files, because Reffitt recorded relevant video files on his Kodak camera and CW-1 saw Reffitt play those videos on the Subject Device.

These facts demonstrate that it is a foregone conclusion that the defendant is the owner of the Subject Device, that he has the ability to decrypt it, and that it stores relevant evidence. "[I]f the respondent's knowledge of the relevant encryption passwords is a foregone conclusion, then the Court may compel decryption under the foregone conclusion doctrine." *Matter of Search of a Residence in Aptos, California 95003*, No. 17-MJ-70656-JSC-1, 2018 WL 1400401, at *6 (N.D. Cal. Mar. 20, 2018), *aff'd by United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018).

CONCLUSION

Wherefore, the government respectfully requests that the Court grant the motion and order the defendant to produce the Subject Device in a decrypted state, first by biometrically unlocking the device with his face and/or irises, and second, if necessary, by typing the password and/or PIN into the keyboard on the Subject Device.

Respectfully submitted,

CHANNING D. PHILLIPS
Acting United States Attorney
DC Bar No. 415793

By: _____
Jeffrey S. Nestler
Assistant United States Attorney
D.C. Bar No. 978296
Risa Berkower
Assistant United States Attorney
NY Bar No. 4536538
U.S. Attorney's Office for the District of Columbia
555 4th Street, N.W.
Washington, D.C. 20530
Phone: 202-252-7277
Email: Jeffrey.Nestler@usdoj.gov

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**Crim. No. 21-cr-00032 (DLF)**
	:	
v.	:	
	:	
GUY WESLEY REFFITT,	:	
	:	
Defendant.	:	

PROPOSED ORDER

Upon consideration of the government's Motion to Compel the Defendant to Produce Evidence in an Unencrypted State, it is hereby ORDERED that:

1. The motion is granted.

2. The defendant is ordered to produce the Microsoft Surface Pro laptop computer (Item 1B20) to the government in an unencrypted state.

3. The government shall proceed in two steps:

   a. *First*, the government shall position the defendant's face in front of the camera of the computer.

   b. *Second*, if the biometric unlock attempt described above does not unlock the computer, the government shall position the defendant and computer so that the defendant can type the password and/or PIN on the keyboard, without the government observing the defendant's keystrokes.

_____

Judge Dabney Friedrich