In the United States District Court
for the District of Kansas

Case No. 20-cr-40068-TC

UNITED STATES OF AMERICA

Plaintiff

v.

JEFFREY DAVID PIERCE,

Defendant

MEMORANDUM AND ORDER

Jeffrey Pierce filed a motion to compel certain information relative to an argument the Government raised in its suppression pleadings. Doc. 40. For the reasons discussed at the May 11, 2021, hearing and as briefly set forth below, that motion is granted in part and denied in part without prejudice.

I

The Government charged Pierce with engaging in a series of electronic communications, mostly by way of his iPhones, that constitute production, possession, and distribution of child pornography (in addition to coercion and enticement of a minor). *See generally* Doc. 25. Pierce moved to suppress the evidence obtained from two of his iPhones because, he contends, agents violated their search warrant by improperly compelling him to involuntarily provide his iPhone passcode. *See generally* Doc. 31. The Government disagrees, arguing that Pierce voluntarily provided the information in a non-coercive setting, they did not violate the warrant's directions, and, even if they had, suppression is unwarranted because agents had access to the code from an independent source (*i.e.*, Pierce's wife, who gave investigators his passcode), they acted in good faith reliance on the warrant, and the information they seek to use is not fruit of the poisonous tree. *See generally* Doc. 37.

This matter arises because of another argument the Government made—inevitable discovery. Essentially, the Government argued that even without the passcode, a law-enforcement-use-only forensic device known as GrayKey would have unlocked or otherwise permitted unfettered access to Pierce's iPhones. Doc. 37 at 36–37 (claiming an ability to obtain 95 percent or more of the data through GrayKey). While more than one software program can deliver those results if an iPhone is in a certain status (known as AFU, which stands for "after first unlock"), Pierce and his consulting expert contend those results are highly questionable when the iPhone is in a different status (known as BFU, which stands for "before first unlock") given the complexity and pervasiveness of Apple's security systems.[1] *See generally* Doc. 40. And, importantly, the Government has provided no evidence that Pierce's iPhones were in the AFU status before the Government used the passcode Pierce provided to unlock the phones. Because of that, he challenges whether the Government's use of GrayKey would have uncovered the same information as opening the phone using his passcode did.

The Government declined Pierce's request to test the alleged efficacy of the GrayKey program. Pierce, therefore, filed a motion to compel the Government to disclose certain materials so that he can independently determine whether the Government's claim—that, even if the phone was in BFU mode, GrayKey would have inevitably led to the discovery of the same information—is valid. Doc. 40 at 4–5 (noting the significant departure GrayKey would be from currently available commercial products).

---

[1] Apple prides itself on iPhone security. Not infrequently, that leads to disagreements with law enforcement entities and, in turn, encourages third-party vendors to provide solutions that are designed to overcome the devices' security measures. *See*, *e.g.*, Nakashima & Albergotti, *The FBI wanted to unlock the San Bernadino shooter's iPhone. It turned to a little-known Australian firm.*, The Washington Post (Apr. 14, 2021) *available at* https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/ (last visited May 11, 2021).

II

Pierce's motion presents two essential questions. One is whether Pierce is entitled to verify the nature of the Government's assertion of inevitable discovery. The other is, if so, how.

A

1. Rule 16 directs that a defendant, upon request, is entitled to inspect documents, data, or tangible things within the government's possession, custody, or control that are "material" to preparing the defense. Fed. R. Cr. P. 16(a)(1)(E); *accord United States v. Simpson*, 845 F.3d 1039, 1056 (10th Cir. 2017). The notions of due process underlying *Brady v. Maryland*, 373 U.S. 83, 87 (1963), reflect a similar obligation that the Government bears.

The Tenth Circuit characterizes information as material when, if disclosed prior to trial, it would have enabled the defendant "significantly to alter the quantum of proof in his favor." *See*, *e.g.*, *United States v. Scott*, No. 92-6272, 1993 WL 411596, at *3 (10th Cir. Oct. 8, 1993) (quoting *United Sates v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975), *cert. denied*, 423 U.S. 836 (1975)). Indeed, that is the standard the Government urges even though all parties agree that the information is being sought in a pre-trial suppression context. Doc. 45 at 12.

The information at issue is material because it will allow Pierce to test the Government's inevitability assertion. The Government, of course, bears the burden of establishing inevitability as an exception to the Fourth Amendment warrant requirement. *See generally United States v. Neugin*, 958 F.3d 924, 932 (10th Cir. 2020). To do so, the Government asserts that the GrayKey device would have inevitably led investigators to the same information as the passcode even if the phone was in BFU mode. That claim, Pierce contends (without meaningful dispute from the Government), is difficult to believe and impossible to verify without the access he is seeking: it is far beyond existing capabilities of other platforms that are publicly available and, as important here, something he cannot verify because GrayKey is available only to law enforcement entities. So, while the Government bears the burden of establishing inevitability, its resistance to Pierce's request precludes him from testing the Government's contention.

The results of the test that Pierce seeks is critical to his defense and his ability to challenge the Government's assertion. As discussed at the

hearing, if the iPhone data is suppressed because the Government cannot establish that GrayKey is capable of inevitably obtaining the data described in its pleadings (and if Pierce manages to prevail on the many other suppression issues regarding the iPhone data seizure, Doc. 37), the quantum of evidence that the Government has against Pierce will be significantly reduced. In fact, Pierce argued at the hearing that the Government would have little, if any, electronic evidence remaining if his motion to suppress is granted.

2. The Government makes three essential arguments against materiality. None are persuasive here.

The Government's lead argument is that the information from GrayKey is not material and should not be given to Pierce because agents did not actually use GrayKey to bypass passcodes on the iPhones. Doc. 45 at 7–12. That argument misses the point: GrayKey's efficacy is relevant not because it was used to access Pierce's iPhones. Its efficacy is relevant because the Government opposed suppression of the iPhone data by arguing that, even if agents improperly obtained the passcode, they would have inevitably obtained the same data by using GrayKey without the ill-gotten passcode. If the Government insists on asserting inevitability based on GrayKey, it must allow Pierce some opportunity to test and verify its claims.

The Government also accuses Pierce of engaging in a fishing expedition. Doc. 45 at 12–14. Not so. Pierce has provided specific, articulable reasons to question GrayKey's abilities and the Government's reliance on them. *See Simpson*, 845 F.3d at 1057–58 (requiring defendants to make a "prima facie showing of materiality" to invoke Rule 16); *United States v. King*, 928 F. Supp. 1059, 1061–62 (D. Kan. 1996) (defining material as "hav[ing] more than an abstract logical relationship to the issues" and emphasizing that the burden is not a heavy one). Thus, Pierce has made the requisite showing of materiality under Rule 16.

The breadth of the material described in Pierce's motion and the extent of proprietary and/or technical details that Pierce's retained digital forensic expert suggests would be useful appears unnecessarily expansive. But the briefs, statements of counsel, and testimony all suggest Pierce is not seeking to obtain access to or possession commercially sensitive or proprietary code. Instead, Pierce's request is merely to test whether, at the time of the events in question, GrayKey was

capable of accomplishing the tasks the Government described to support its inevitable discovery argument.

Finally, the Government contends that its obligation to disclose information at a suppression hearing is less demanding than it would be at trial. Doc. 45 at 14–15. That argument misses the mark. The Government put this evidence at issue and bears the burden of establishing inevitability at the suppression hearing. Despite that, it is precluding Pierce from verifying—or effectively disproving—its contentions.

* * *

In conclusion, Pierce is entitled to test the Government's inevitability argument. The information being sought is material to Pierce's ability to defend against these serious charges, and the Government's arguments to the contrary are insufficient to justify a different result.

B

Determining how best to afford Pierce access to the data he seeks while protecting the significant interests described by the Government presents a more complex and nuanced problem. It is not entirely clear that law enforcement privilege applies to the GrayKey product,[2] but

[2] It is not settled that a device such as GrayKey is entitled to the law enforcement privilege. *Compare United States v. Roviaro*, 353 U.S. 53 (1957) (recognizing such privilege only for the identities of confidential informants) *with United States v. Van Horn*, 789 F.2d 1492 (11th Cir. 1986) (extending the privilege to surveillance equipment); *see also* Doc. 45 at 16–18 (identifying no Tenth Circuit precedent suggesting that it applies to GrayKey or similar devices). Even where such privilege applies, it is strictly limited to situations where the government's interest in "protecting the flow of information" outweighs the "individual's right to prepare his defense," taking into consideration "the crime charged, the possible defense, the possible significance of the [evidence at issue], and other relevant factors." *Roviaro*, 353 U.S. at 62. Here, Pierce is charged with extremely serious crimes, he is facing significant punishment, and excluding evidence from his iPhones is significant to his defense. The risk of infringing the Government's interest in protecting information is low, given that limitations on the scope of production and appropriate protective orders can adequately protect the information against malicious actors. Where there is any question about the balance of these factors, the "privilege must give way" to the accused's defense. *Id.* at 60.

even if it does not, the technology is sufficiently sensitive that (as Pierce recognizes) his scope of access should reflect that sensitivity. Much time was spent at the hearing exploring the practical difficulties of crafting such an order designed to provide appropriately limited yet meaningful access. Many of the issues relevant to that inquiry implicate complicated technical issues (that affect everything from logistics to timing to format), unresolved deliberations on how to permit limited yet meaningful access to the data, and how to do so within the Government's contractual obligations to GrayKey's creator, Grayshift.

The parties are encouraged to explore cost-efficient means to allow Pierce sufficient access to be able to test the Government's inevitability claim. At the same time, other interests are at play that must also be accomodated. *See generally* Doc. 45 at 15–25. This Order should not be read to suggest that all of what Pierce's motion sought should be provided. Many alternatives were discussed but not fully explored at the hearing, including the possibility of Pierce's expert observing governmental agents demonstrating GrayKey's capability so that neither GrayKey's software nor hardware leave the pertinent law enforcement office.

A status conference was previously set for July 14, 2021. If the parties are able to agree on the scope of Pierce's GrayKey review, they may file a pleading to that effect and request that the status conference occur by telephone for the limited purpose of setting a suppression hearing. If the parties are unable to reach such an agreement, each party shall file, at least one week before the hearing, a proposal on the best way to provide Pierce limited but meaningful access to the inevitability data, and counsel should appear in person as scheduled to resolve that issue.

III

For the foregoing reasons, Pierce's motion to compel, Doc. 40, is granted in part and denied in part without prejudice.

It is so ordered.

Date: May 14, 2021

s/ Toby Crouse
Toby Crouse
United States District Judge