UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DENNIS COLLINS, CHRISTOPHER WAYNE COOPER, JOSHUA JOHN COVELLI, KEITH WILSON DOWNEY, MERCEDES RENEE HAEFER, DONALD HUSBAND, VINCENT CHARLES KERSHAW, ETHAN HAINDL MILES, JAMES C. MURPHY, DREW ALAN PHILLIPS, JEFFREY PUGLISI, DANIEL SULLIVAN, TRACEY ANN VALENZUELA, CHRISTOPHER QUANG VO, Defendants.	Case No.: 11-CR-00471-DLJ (PSG) **ORDER RE PRETRIAL CONDITIONS AND GOVERNMENT'S DISCOVERY OBLIGATIONS** **(Re: Docket Nos. 174, 191, 192, 202, 206, 207)**

The 14 defendants in this case were indicted on July 13, 2011 on 15 counts of conspiracy to cause damage to a protected computer and aiding and abetting causing intentional damage to a protected computer, in violation of 18 U.S.C. § 1030. The indictment alleges that in retribution for PayPal, Inc.'s termination of WikiLeaks.org's donation account, the defendants and other members of a group calling itself Anonymous coordinated and executed distributed denial of service (DDoS) attacks against PayPal's computer servers using the "Low Orbit Ion Cannon" open source computer application the group makes available for free download on the internet. According to the indictment, in late November 2010, WikiLeaks released a large amount of classified United

States State Department cables on its website. Citing violations of the PayPal terms of service, and in response to WikiLeaks' release of the classified cables, PayPal suspended WikiLeaks' accounts so that WikiLeaks could no longer receive donations.

On September 1, 2011, the defendants made their initial appearance in this court and were arraigned. Each defendant consented to pretrial release under a number of conditions, including conditions that each defendant (1) not participate in or accessing Internet Relay Chats ("IRCs"); (2) not use or access Twitter; (3) designate the computer or computers that would be used while on release; (4) not delete any internet history; and (5) make available any designated computer for inspection by Pretrial Services.[1]

On February 17, 2012, the parties appeared for a hearing on a variety of disputes regarding the release conditions and discovery. These disputes are addressed in the following pleadings pursuant to Fed. R. Crim. P. 16 and 18 U.S.C. § 3142: Kershaw's Motion to Modify Mr. Kershaw's Pretrial Release Conditions (Docket No. 174); Defendant Tracy A. Valenzuela's ("Valenzuela") Objection to Request of Pretrial Services Set Forth In the Memoranda Dated January 31, 2012 (Docket No. 191); Valenzuela's Motion to Compel the Government to Produce Information Responsive to the Warrants (Docket 192); Defendant Christopher W. Cooper's ("Cooper") Response to Pretrial Services' Notice of Bail Violation (Docket No. 202); Defendant Christopher Q. Vo's Objection to Pretrial Services' Recommendation and Motion to Modify Conditions of Release (Docket No. 206); and Kershaw's Motion to Reject Proposal of Pretrial Services to Change Conditions of Release (Docket 207).

Having considered the arguments of the parties and the applicable law, the court rules as follows:

1. The restriction on each defendant's deletion of internet history shall be modified to restrict only intentional deletion.

2. The inspection condition shall be modified to:

[1] *See, e.g.*, Docket No. 122 (Order Setting Conditions of Release for Dennis Collins). The court notes that while Defendant Vincent Charles Kershaw ("Kershaw") later rejected the proposed condition restricting his use of IRC and Twitter.

a. The defendant shall submit any designated computer for inspection as directed by Pretrial Services;

b. Pretrial Services shall use any appropriate method available to monitor the defendant's computer usage. The defendant shall cooperate with Pretrial Services and provide information about which computer programs are installed on any designated computer;

c. The defendant shall surrender the computer to Pretrial Services (if necessary for the inspection) and it shall be returned promptly to the defendant after the computer inspection has been completed; and

d. Pretrial Services has the discretion to allow the defendant to be present during the inspection of any designated computer.

3. The restriction on each defendant's use of or access to Twitter shall be deleted.

4. The inspection condition on Kershaw's alcohol use shall be modified to restrict only excessive alcohol use.

5. No later than 30 days from the date of this order, the government shall return all data outside the scope of the warrants.

All other requested relief is denied.

I. INSPECTION BY MONITORING

Various defendants request modification of the court's condition in its release orders that each defendant make available for inspection by Pretrial Services any computer designated for use. The defendants' request is in response to various reports from Pretrial Services that officers in nine of the 13 judicial districts responsible for supervising the defendants could not effectively implement the inspection condition as ordered without installing monitoring software.[2] These officers explained that, in the absence of any monitoring program installed either on the computer's

[2] The Pretrial Services reports included a December 7, 2011 report regarding the supervision of Defendant Ethan Miles ("Miles") in District of Arizona and a December 20, 2011 report regarding the supervision of Cooper in the Southern District of Alabama. The December 20 report noted that Cooper was found to have run a commercial virus and malware scanning computer program on a designated computer that deleted the computer's internet history in order to restore the computer's performance.

hard drive or by USB drive, they could only enforce the inspection condition by manual searches. These officers further explained manual searches were subject to a host of limitations, including the time to conduct the search, potential inconsistencies from search to search, and an overnight drop-off requirement in some districts that conflicted with the release order provision that each defendant be permitted to be present during any inspection. The defendants object to any hard drive installation of the software, arguing that installed monitoring software unduly burdens their privacy and that if the inspection condition is appropriately maintained at all, it should be enforced only by a USB drive loaded with "Fieldsearch," a scanning program supplied by the National Law Enforcement and Corrections Technology Center ("NLECTC").[3] The defendants also urge the release conditions be modified to clarify that only "intentional" deletion of internet history is prohibited.

The government responds that it does not object the defendants' use of anti-virus software. At the same time it reiterates the need to monitor internet activity in light of the computer fraud allegations set forth in the indictment and opposes any deletion of the inspection condition.

Particularly in the absence of any real objection by the government, the court is persuaded that the latter modification proposed by the defendants is appropriate. Intentional, not inadvertent, deletion of internet history thwarts the government's legitimate interest in assuring that a defendant does not violate internet activities otherwise prohibited by the release order.

The court is not persuaded, however, that the former modification proposed by the defendants is similarly appropriate. What defendants ask is for this court to compel the deployment of technology by Pretrial Services in this district and over a dozen others. As a matter of comity alone, to say nothing of its limited authority and jurisdiction, the court will not presume to dictate to other federal district courts how to supervise defendants under their charge.

Even as to this district, the court is not persuaded to mandate inspection by a given software program. The court is aware that only recently, the Ninth Circuit again acknowledged that "monitoring software and/or hardware takes many forms, with greatly varying degrees of

[3] NLECTC also has produced a training manual and video for the program. *See* https://fieldsearch.justnet.org.

intrusiveness."[4] While the experience reported by Cooper's supervisory officer in the Southern District of Alabama suggests that Fieldsearch can be an effective tool, the literature about the program supplied by Cooper identifies a number of limitations. For one thing, while Microsoft Windows and Apple Macintosh versions are available, the program may not be used on any computer running the Linux operating system. For another, the program is supplied with training materials necessary for even basic instruction that have not yet been made available in this district. The court is aware of no statute or case, and the defendants have not supplied any, suggesting that in setting the "least restrictive conditions necessary to secure each defendant's appearance and to protect the safety of the community,"[5] a court may not delegate to its Pretrial Services department the discretion to determine which particular technology is to be used.[6]

The better course is to delegate to Pretrial Services in this and other districts the discretion to inspect each defendant's designated computer as it deems appropriate-- whether by Fieldsearch, hardware installation of an alternative program, or manual searching-- so long as it is does so consistent with the court's mandate in setting the condition and is "reasonably calculated to fulfill" the purpose of the condition.[7] To accomplish this, the court will modify the inspection condition largely as proposed by Pretrial Services. At the same time, and "complementary to that delegation," Pretrial Services is under "a continuing obligation to ensure not only the efficiency of computer surveillance methods used, but also that they remain reasonably tailored so as not to be unnecessarily intrusive."[8] While the court is mindful of the defendants' legitimate privacy

---

[4] *United States v. Quinzon*, 643 F.3d 1266, 1271 (9th Cir. 2011) (quoting *United States v. Sates*, 476 F.3d 732, 737-38 (9th Cir. 2007)).

[5] 18 U.S.C § 3142(c)(1)(B).

[6] In fact, in the admittedly different context of post-conviction supervision, the Ninth Circuit has explicitly affirmed that a district court may "leave to [a] probation officer the details of what technologies should be used.'" *Quinzon*, 643 F.3d at 1274. *See also United States v. Stephens*, 424 F.3d 876, 883-84 (9th Cir. 2005) (acknowledging that district courts may delegate to probation officers the task of choosing particular drug or psychological programs). *Cf. United States v. Benatar*, Case No. 02-CR-99, 2002 WL 31410262, at *3 (E.D.N.Y. Oct. 10, 2002) (rejecting literal reading of the Bail Reform Act that would require release no matter what the cost of conditions to be supervised by Pretrial Services).

[7] *See Stack v. Boyle*, 342 U.S. 1, 5, 72 S.Ct. 1, 96 L.Ed. 3 (1951).

[8] *United States v. Quinzon*, 643 F.3d at 1271.

concerns, as arrestees they enjoy "a lesser privacy interest than the general population."[9] The court is satisfied that Pretrial Services can take sufficient steps to mitigate the risk of unauthorized disclosure, as it does regularly in this case and others in managing highly sensitive information such as drug testing data. To the extent new technologies emerge or circumstances arise demonstrating that the monitoring implemented by Pretrial Services is falling short of these requirements, any party may again request modifying the condition.

II. RESTRICTION ON IRC AND TWITTER

Kershaw and other defendants request that the Court modify the release orders to delete the prohibition against participation in or accessing of IRC and use of or access to Twitter. Kershaw argues that the IRC and Twitter restrictions violates his right to freedom of speech under the First Amendment. The crux of Kershaw's argument is that the restriction unduly burdens his right to engage in political discourse by these means. Kershaw points out that the ban denies him tweets issued by President Obama and other national figures and prevents him from engaging in Twitter Town Halls. Kershaw makes similar points regarding the ban on use of IRC and notes that the monitoring condition provides a sufficient means to assure that his Twitter and IRC activities do not threaten public safety or somehow facilitate his flight from prosecution.

The government responds with a general proffer that the conspiracy in which each defendant is alleged to have participated was coordinated by IRC and Twitter communications. The government further notes that the IRC and Twitter restrictions leave available to Kershaw and the other defendants any number of alternative means of engaging in political discourse.

The court sees no constitutional deprivation in the IRC restriction currently in place. As an initial matter, the court notes that the defendants do not challenge the IRC and Twitter restrictions as deprivations of due process or excess bail.[10] Case law addressing the limits on pretrial release

---

[9] *Haskell v. Brown*, 677 F.Supp.2d 1187, 1197 (N.D. Cal. 2009). *See also United States v. Kincade*, 379 F.3d 813, 864 (Reinhardt, J. dissenting) (noting that arrestees' privacy interests appear to be "significantly reduced").

[10] *Cf. United States v. Salerno*, 481 U.S. 739, 745, 107 S.Ct. 2095, 95 L.Ed.2d 697 (1987) (recognizing that federal bail provisions are subject to constitutional limitations of due process and excessive bail); *Bell v. Wolfish*, 441 U.S. 520, 535, 99 S.Ct. 1861, 60 L.Ed.2d 447 (1979)

conditions imposed by the First Amendment is limited, and indeed the parties have brought no such opinions to the court's attention. It nevertheless appears clear that the First Amendment can restrict pretrial conditions imposed on defendants[11] and that in this circuit even the defendants other than Kershaw who consented to release on conditions did not waive their right to challenge those conditions on constitutional grounds.[12]

"Without question, a defendant who is under court supervision, including based upon a conditional pretrial release order, does not necessarily forfeit all of his or her First Amendment rights. Consequently, in fashioning suitable conditions to govern the defendant's release pending trial on the various charges against him in this case, the court [is] required to do so in a manner which would result in no greater intrusion upon defendant's constitutional rights, including those guaranteed under the First Amendment, than reasonably necessary in order to effectuate the objectives of the Bail Reform Act, and to additionally insure defendant's compliance with the court's order."[13] While any limitation on free speech must be imposed cautiously, and each defendant retains the presumption of innocence during the pretrial period,[14] the IRC restriction in this case furthers a compelling government interest in protecting the public from further crimes coordinated through a means specifically addressed by the grand jury in the language of the indictment.[15] The condition operates in a content-neutral fashion. The condition does not restrict political or any other discourse by any other means, even by use of other internet services such as email, blogging services such as Tumblr, chat other than IRC, or social networks such as Facebook

---

("[C]onditions or restrictions of pretrial detention ... implicate ... protection against liberty without due process of law.").

[11] *See, e.g.*, *Bell*, 441 U.S. at 545.

[12] *See United States v. Scott*, 450 F.3d 853, 865-67 (9th Cir. 2006).

[13] *United States v. Murtari*, Case Nos. 5:07-CR-0428 (DEP), 5:07-CR-406 (DEP), 5:08-CR-0059(DEP), 5:08-CR-0060 (DEP), 2008 WL 687434, at *4 (N.D.N.Y. Mar. 11, 2008).

[14] *See* 18 U.S.C. § 3142(j).

[15] *See* Docket No. 1 (Indictment) at 3.

or Google+.[16] All of this suggests to the court that a restriction on IRC use, while permitting substantial internet use for purposes that include political discourse, strikes a reasonable balance between the legitimate and yet competing interests of the parties.

The court is not persuaded, however, that the restriction on Twitter use should be maintained. The indictment makes no mention of Twitter whatsoever. While the government's general proffer mentions Twitter, and courts regularly approve proceeding in detention proceedings by way of proffer,[17] nothing proffered by the government sufficiently links any defendant's allegedly criminal activities to use of a Twitter account. In the absence of any indictment charge, any evidence, or even any specific proffer of such illicit activity by Twitter, the court is not persuaded that the restriction advances any legitimate interest in protecting the public's safety or prevent any defendant from fleeing. Under these circumstances, any illicit use of Twitter by any defendant may be adequately addressed by the monitoring approved elsewhere in this order.

III. URINE ANALYSIS AND RESTRICTION ON EXCESSIVE ALCOLHOL USE

Kershaw requests that the Court modify his release order to delete his urine analysis condition. Kershaw argues that there is no indication that he suffers from any narcotic addiction or abuse.

The government responds that the probation officer supervising Kershaw's pretrial release has reported that Kershaw suffers from an alcohol addiction. Kershaw has reported that he has consumed alcohol even while returning from an alcohol treatment class and after consuming Antabuse, which causes a severe negative physical reaction to alcohol intake.

Under many circumstances similar to this, where the court is presented with a proffer of evidence of a substance addiction, the court approves a testing condition. Congress has explicitly approved an appropriate restriction on excessive alcohol and controlled substance use,[18] and as

---

[16] *Cf. City Council of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 812 (1984) ("the First Amendment does not guarantee the right to employ every conceivable method of communication at all times at all places."). The court also notes that the condition does not impose any burden greater than associational and other First Amendment-impacted restrictions routinely imposed by courts as a condition of pretrial release. *See, e.g., United States v. Spilotro*, 786 F.2dd 808, 815-816 (8th Cir. 1986).

[17] *See United States v. Corderas*, 784 F.2d 937, *vacated as moot*, 792 F.2d 906 (9th Cir. 1986).

[18] *See* 18 U.S.C. § 3142(c)(1)(B)(ix).

discussed below a restriction on excessive alcohol use by Kershaw is warranted. Testing in furtherance of such a condition here appears not only warranted, but wise. This request is denied.

IV. ANTABUSE REQUIREMENT

Kershaw requests that the Court modify his release order to prohibit any requirement that he consume Antabuse. He notes that if the court wishes to restrict his excessive consumption of alcohol, it should do directly rather than by requiring him to ingest medication that causes him serious side effects, including sleepiness, vision problems and headaches.

The government disputes that any condition in Kershaw's release order requires him to take Antabuse. According to the government, Kershaw's probation officer merely suggested that Kershaw consider Antabuse in order to improve his odds of complying with the release order's restriction on alcohol use.

The court finds no requirement that Kershaw take Antabuse, and declines to impose this requirement now. The court will instead modify Kershaw's release order to prohibit excessive, rather than any, alcohol use. Kershaw should note, however, that any violation, let alone repeated violations of this restriction on excessive alcohol use puts him at substantial risk of revocation and remand to custody.

V. THE GOVERNMENT'S DISCOVERY OBLIGATIONS

On January 27 and 28, 2011, several months before the indictment issued in this case, the government executed 27 search warrants by which it seized from the defendants over 100 computers and other digital devices (including storage media). To date, none of the data files on these devices justifying the warrants has been tendered to the defendants nor have any of the devices been returned.

Various defendants request that the government segregate all information within the scope of the warrants upon which the government relied in seizing any device, distribute that information to all defendants in accord with a protocol agreed to by the parties, and return all devices and non-targeted data to the defendants from whom they were seized without further delay. In arguing for the separation and production of data and return of their non-targeted data and devices, the defendants principally rely on (1) statements made by Judge Jensen at a November 1, 2011 status

conference observing that the government may only keep targeted data in its possession and (2) language in the warrants themselves that compels the return, deletion of destruction of any data outside the scope of the warrant unless otherwise provided by law.

The government responds that under the terms of Schedule C of various of the warrants it may retain the devices seized as forfeitable instrumentalities of the criminal offenses alleged. The government further argues that it may keep a complete forensic copy of an image of each device in order to link each seized device and the evidence contained on it to a particular defendant, and to rebut any claim by the defendants that the device has been modified or altered in any way. The government finally argues that it satisfied its obligation to produce all targeted data by tendering complete forensic images to the parties' discovery coordinator, who can then distribute the data of each defendant upon his consent.

Before addressing the merits of the parties' requests, the court notes that Judge Jensen's statements regarding the government's discovery obligations appear preliminary in nature. No request for an order was pending before him and no party appears to have briefed the issues now in dispute. The court will nevertheless now consider to the disputed issues with the guidance of the presiding judge firmly in mind.

Beginning with the issue of the seized devices, the court notes that returns of seized property are typically presented by way of a motion pursuant to Fed. R. Crim. P. 41(g). Even where no indictment has issued, a party simply looking to get its property back from the government may initiate a civil equitable proceeding applying the principals of Rule 41(g).[19] But even though the defendants do not explicitly invoke Rule 41(g), it is difficult to understand the defendants' request for the return of their devices as anything other than a Rule 41(g) motion. In this setting, the court must be mindful of the limitations on its authority and jurisdiction under both 28 U.S.C. § 636(b) and this court's General Order 42. Section 636(b) does not identify any authority for this court to rule on any motion for return as a non-dispositive motion, and General Order 42 explicitly prohibits preparation by a magistrate judge of a report and recommendation on a dispositive

[19] *See, e.g., Ramsden v. United States*, 2 F.3d 322, 324-25 (9th Cir. 1993).

motion. The court has failed to identify any Ninth Circuit case characterizing a Rule 41(g) motion as non-dispositive, but must conclude that a magistrate judge's consideration of a Rule 41(g) motion is appropriately treated as a report and recommendation on a dispositive motion. Because such consideration is precluded in this district by General Order 42,[20] the undersigned must decline either to rule on the requested return of the defendants' devices or even to issue a formal recommendation on the subject.[21]

Turning to the government's obligation to segregate and disclose data seized in support of its investigation and prosecution,[22] this Circuit has long held that the government is precluded from keeping seized documents that are outside the scope of the warrant.[23] This basic principle was only recently affirmed by the Ninth Circuit in the specific context of electronic documents seized from computers and other storage media.[24] Many of the warrants in this case specifically acknowledge the government's return obligation by providing that "[w]ithin a reasonable period of time, but not

---

[20] *See* General Order 42 at ¶ 3 ("Case dispositive matters in criminal felony cases including motions to dismiss an indictment or information made by a defendant or to suppress evidence").

[21] The court can note, however, even if the seized devices were properly removed from the searched premises as instrumentalities subject to forfeiture, there appears to be no support for the notion that the government may thereafter hold on to the devices without any foreseeable end. The more appropriate course would appear to be for the government to return each of the devices for which the government is unable to tender evidence supporting its claim that the device was used to commit a crime at issue. *See generally*, Orin Kerr, *Search Warrants In An Era of Digital Devices*, 75 Miss.L.J. 85, 131 (2005). This is especially so more than a year after the devices were seized and presumably subjected to forensic copying and analysis and in the absence of any forfeiture allegation in the indictment.

[22] This obligation may arise under the Jencks Act, 18 U.S.C. § 3500, *Giglio v. United States*, 405 U.S. 150 (1972) or *Brady v. Maryland*, 373 U.S. 83 (1963).

[23] *See United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982). In considering the standards for discovery of electronic data in criminal cases, at least one other district court has looked to the principals applicable in civil case under Fed. R. Civ. P. 34. *See United States v. O'Keefe*, 537 F.Supp.2d 14 (D.D.C. 2008). But this court is not persuaded that the leap between criminal and civil in this context is appropriate. Civil cases generally require broad discovery on the basis of relevance. In contrast, in criminal cases the government's duty to disclose is much more limited and extends only to items such as material exculpatory and impeachment information, witness statements, and a defendant's statements and prior record.

[24] *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1170-77 (9th Cir. 2010) ("*Tamura* has provided a workable framework for almost three decades, and might well have sufficed in this case had its teachings been followed. We have updated *Tamura* to apply to the daunting realities of electronic searches").

to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain the data." While the government emphasizes the final clause of this provision, even if the law ultimately permits the forfeiture of a given device as discussed above, under *Tamura* and *CDT* the law does not permit the retention of data on that device that has not been shown or even alleged to have been an "instrumentality" of the alleged crimes. Nor does the law permit the retention of data outside the scope of the warrant for identification, authentication or chain-of-custody purposes. That argument has been specifically rejected in this district in *United States v. Lu*: "[t]he government, however, shall not be retaining images of file documents that, in large part, do not contain information within the scope of the warrant."[25]

In sum, after considering the arguments of the parties and the applicable case law, the undersigned ultimately returns to the preliminary assessment of the presiding judge: the government has no claim to data outside the scope of the warrant. By some other reasonable effort that minimizes the government's exposure to non-targeted documents,[26] no later than 30 days from the date of this order, the government must endeavor to give back to the defendants data outside the scope of the warrants. In making the targeted data available to the defendants, the government is urged to heed the instruction of any number of cases on the subject that a production of a

[25] Case No. CR 09-00341 RMW (N.D. Cal. Sept. 9, 2010) (Docket No. 12 at 4 (citing *Tamura*)).

[26] *See, e.g., United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d at 1178-80 (Kozinski, J., concurring) (outlining the parameters of "search protocol reasonably structured to prevent agents involved in the investigation from examining or retaining any data other than for which probable cause is shown").

searchable database can avoid subsequent challenges under Rule 16, *Brady*, and *Giglio*.[27]

IT IS SO ORDERED.

Dated: 3/16/2012

PAUL S. GREWAL
United States Magistrate Judge

[27] *See, e.g.*, *United States v. Skilling*, 557 F.3d 529, 575, 577 (5th Cir. 2009); *United States v. Warshak*, 631 F.3d 266, 297 (6th Cir. 2010); *United States v. Ohle*, 08-CR-1109 (JSR), 2011 WL 651849, at *3-4 (S.D.N.Y. Feb. 7, 2011).