FILED
United States Court of Appeals
Tenth Circuit

May 19, 2009

Elisabeth A. Shumaker
Clerk of Court

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. FRANCISCO L. MATTESON, Defendant-Appellant.	No. 08-2176 (D.C. No. 1:07-CR-805-JCH-1) (D.N.M.)

ORDER AND JUDGMENT[*]

Before **BRISCOE**, **EBEL**, and **GORSUCH**, Circuit Judges.

In May 2005, New Mexico authorities arrested Francisco Matteson for defrauding various banks. Mr. Matteson admits that he stole mail in order to obtain personal information and bank account numbers belonging to at least eighty-nine people. Using this stolen information along with his personal computer and other equipment perhaps belonging to another individual, Mr. Matteson produced counterfeit checks that he sold for cash. Under an agreement with the government, Mr. Matteson pled guilty to one count of possession of stolen mail, 18 U.S.C. § 1708, and another count of bank fraud, 18 U.S.C.

---

[*]This order and judgment is not binding precedent except under the doctrines of law of the case, res judicata and collateral estoppel. It may be cited, however, for its persuasive value consistent with Fed. R. App. P. 32.1 and 10th Cir. R. 32.1.

§ 1344(1)-(2). The district court sentenced him to thirty-three months' imprisonment followed by a three year term of supervised release.

This appeal concerns one of the special conditions of supervised release imposed by the district court. The district court is invested with broad discretion to prescribe such conditions, subject to the limitations imposed by law, including 18 U.S.C. § 3583(d). *United States v. Hanrahan*, 508 F.3d 962, 970 (10th Cir. 2007). Section 3583(d) requires, among other things, that any special condition be reasonably related to certain factors set out in 18 U.S.C. § 3553(a), including "the nature and circumstances of the offense and the history and characteristics of the defendant," as well as three purposes of punishment: deterring criminal conduct, protecting the public, and providing the defendant with training, medical care, and other correctional treatment. 18 U.S.C. § 3583(d)(1); *id.* § 3553(a)(1), (a)(2)(B)-(D). The condition must also "involve[] no greater deprivation of liberty than is reasonably necessary" to achieve those three purposes. *Id.* § 3583(d)(2).

In our case, the challenged condition provides that

> [t]he defendant shall consent, at the direction of the United States Probation Officer, to having installed on his/her computer(s), any hardware or software systems to monitor his/her computer use. The defendant understands that the software may record any and all activity on his/her computer, including the capture of keystrokes, application information, Internet use history, e-mail correspondence, and chat conversations. Monitoring will occur on a random and/or regular basis. The defendant further understands that he/she will warn others of the

> existence of the monitoring software placed on his/her computer *or any such computer* [to which] *the defendant may have access*.

D. Ct. Judgment at 4 (emphasis added).

Before us, Mr. Matteson argues that this condition is problematic in two respects. First, he claims that the condition (in particular, the italicized language) is impermissibly vague. Second, he contends that the level of monitoring authorized (down to the last keystroke) is too intrusive to comply with § 3583(d) or the Fourth Amendment. Because Mr. Matteson raised neither argument to the district court, normally our review would be for plain error.

In this case, however, the government has commendably conceded Mr. Matteson's first, vagueness argument. In light of this concession, "the question of whether we apply plain error review" with respect to that argument is not "trigger[ed]." *United States v. White*, 244 F.3d 1199, 1207 n.11 (10th Cir. 2001). As counsel for the government rightly pointed out in a letter to us, it is unclear from the terms of the district court's condition whether that court intended to authorize the government to monitor not just Mr. Matteson's computer, but also any other computer to which he might have access. The first part of the district court's condition authorizes monitoring only on "his[] computer(s)." By contrast, the last sentence of the court's condition imposes an obligation on Mr. Matteson to "warn others" that the monitoring software has been placed on his computer "or any such computer [to which] the defendant may have access." As the

government acknowledges, it is possible that the district court did not mean to require monitoring of any computers beyond those owned by Mr. Matteson. *See* United States' Letter of March 19, 2009, at 2. But it is also possible that the district court intended in the final words of the condition to expand the number of monitored computers. Indeed, the government submits this is the more plausible reading of the district court's intentions for two reasons: first, the alternative renders the last eleven words of the special condition superfluous; second, the evidence in this case suggested a need to encompass more than just computers belonging to Mr. Matteson because he "committed the offense using both his own computer and a borrowed computer." *Id.* In any event, both sides before us agree a remand is necessary to clear this up.

While conceding Mr. Matteson's first argument about the vagueness of the district court's condition, the government nonetheless urges us to reject Mr. Matteson's second argument, at least in part. Specifically, the government asks us to affirm keystroke monitoring of those computers owned by Mr. Matteson, arguing that such a requirement would not offend § 3583(d)(2)'s requirement of impinging no more than is reasonably necessary on Mr. Matteson's liberty.

We think the better course in this particular case is to defer resolution of this question until after remand. It may be that the district court wishes keystroke monitoring to apply only to computers owned by Mr. Matteson, while other computers Mr. Matteson uses (such as those owned by an employer) are subject

either to no monitoring at all or to some other, less intrusive and as yet unspecified form of monitoring. But, again, it could be the intent of the condition to require keystroke monitoring of *all* computers Mr. Matteson uses, not just those he owns. And it is difficult to evaluate the propriety of the district court's keystroke monitoring requirement as a whole without first knowing to which computers it pertains; what might be sustainable in isolation might become unsustainable when the condition is viewed as a whole. Underscoring this is the fact that the government itself has suggested not only that the district court most likely wished its condition to apply to any computer Mr. Matteson might access, but also that, if the keystroke monitoring requirement does pertain so broadly, it is "too broad" for us to sustain. United States' Letter of March 19, 2009, at 2. Rather than evaluating this case piecemeal, and doing so based on hunches about the district court's intentions and what might ultimately prove sustainable, we believe the district court should have a chance in the first instance to think comprehensively about which conditions it wishes to impose, if any, on which computers. After the district court's evaluation, the case may look very different than our assumptions now suggest.

Our decision to wait for the district court's evaluation in the first instance is also influenced by the fact that determining the boundaries of permissible computer monitoring has vexed several of our sister circuits, and our circuit has not yet issued comparable guidance. *Compare United States v. Sales*, 476 F.3d

732, 737-38 (9th Cir. 2007) (vacating computer monitoring as not narrowly tailored); *United States v. Lifshitz*, 369 F.3d 173, 192-93 (2d Cir. 2004) (vacating and remanding computer monitoring condition to permit district court to evaluate potential overbreadth in the first instance), *with United States v. Goddard*, 537 F.3d 1087, 1090-91 (9th Cir. 2008) (monitoring condition valid if narrowly construed); *United States v. Holm*, 326 F.3d 872, 879 (7th Cir. 2003) (random searches of probationer's computer "entirely reasonable"). Before weighing in on this weighty subject for the first time, we would no doubt benefit not just from a clearer understanding of what we are being asked to review, but also from the district court's considered views on how its conditions mesh with and are tailored to both § 3583(d)(2)'s requirements and the Fourth Amendment.

The challenged condition of supervised release requiring computer monitoring is vacated in its entirety, and the case is remanded for further proceedings consistent with this order.

ENTERED FOR THE COURT

Neil M. Gorsuch
Circuit Judge