

FILED

APR 03 2018

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ARMEN BISLAMIAN, AKA Eric Doski,

Defendant-Appellant.

No. 16-50106

D.C. No. 2:14-cr-00494-PA-1

MEMORANDUM*

Appeal from the United States District Court
for the Central District of California
Percy Anderson, District Judge, Presiding

Argued and Submitted February 15, 2018
Pasadena, California

Before: BERZON and BYBEE, Circuit Judges, and GLEASON,** District Judge.

Defendant Armen Bislamian appeals the imposition of three computer and Internet search and monitoring conditions attached to his supervised release. He maintains that the conditions are neither sufficiently narrowly tailored nor

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The Honorable Sharon L. Gleason, United States District Judge for the District of Alaska, sitting by designation.

reasonably related to his conviction for conspiracy to commit bank fraud, and so, under 18 U.S.C. § 3583(d), must be vacated. We disagree and affirm.

1. As Bislamian concedes, he did not object to the three conditions before the district court. We therefore may vacate the conditions only if their imposition was in plain error. *United States v. LaCoste*, 821 F.3d 1187, 1190 (9th Cir. 2016).

We conclude that any potential error by the district court in this case was not plain, “clear[,] or obvious.” *United States v. Wolf Child*, 699 F.3d 1082, 1095 (9th Cir. 2012) (internal quotation marks omitted). Bislamian used various pieces of digital technology to commit his crime: a “skimming device,” credit card encoding equipment, data storage devices, and a personal computer. The district court thus could have found a “reasonabl[e] relat[ionship]” between Bislamian’s crime and criminal history, on the one hand, and the computer and computer-related devices subject to search and seizure, on the other. 18 U.S.C. § 3583(d)(1).

The record does not definitively indicate that Bislamian used the Internet to commit his crime, but the district court could have inferred as much. Bislamian admitted to “obtain[ing] additional victim account holders’ information, including credit profiles and zip codes, in order to facilitate the use of the re-encoded [fraudulent] cards.” It would be reasonable to infer that Bislamian did so using the Internet, or would do so in the future using the Internet, as non-Internet sources for

the information obtained would be considerably more difficult to access. Given that reasonable inference, the Internet monitoring conditions were “reasonably related” to Bislamian’s crime and “involve[d] no greater deprivation of liberty than [wa]s reasonably necessary.” 18 U.S.C. § 3583(d)(1), (d)(2); *cf. United States v. Bare*, 806 F.3d 1011, 1017-20 (9th Cir. 2015).

2. Bislamian points to two cases—*United States v. Sales*, 476 F.3d 732 (9th Cir. 2007), and *United States v. Barsumyan*, 517 F.3d 1154 (9th Cir. 2008)—and maintains that they “make clear that it is improper to impose computer and Internet restrictions where the underlying offense was not the direct result of using the Internet.” Those cases do not make that point sufficiently clear to warrant reversal on plain error review.

Barsumyan vacated a condition of supervised release under which the defendant was prohibited from *accessing* “any computer or computer-related devices in any manner . . . unless approved in advance.” 517 F.3d at 1157. All that *Barsumyan* made “clear” was that “a mere nexus between the crime and a computer does not justify *proscribing* the use of *anything* containing a circuit board or microchips.” *Id.* at 1161 (emphasis added and footnote omitted). This case concerns something else: *searches* of computers via real-time monitoring, not prohibitions or restrictions on their use. “While we have on occasion vacated

conditions of supervised release limiting or restricting the ability to use computers and access the Internet, we have not taken such a heavy hand with respect to general search conditions of personal computers.” *Bare*, 806 F.3d at 1017.

Similarly, *Sales* does not plainly require reversal. In *Sales*, aside from the defendant’s use of his personal scanner and printer, “his unlawful activity did not utilize any other devices, and in no way involved or relied upon the internet, electronic bulletin boards, or other networks.” 476 F.3d at 736. The court reasoned that, as to a computer monitoring condition imposed on the defendant, “further tailoring and clarification [were] required” in light of the fact that the monitoring apparently extended to any device used by the defendant “for work or personal purposes,” whether or not he owned the device. *Id.* at 737. The monitoring condition was also “overbroad in other respects”: “[T]o comply with the Fourth Amendment, it must be narrowly tailored,” yet “the text g[ave] no indication as to what kinds or degrees of monitoring [were] authorized,” despite the fact that “monitoring software and/or hardware takes many forms, with greatly varying degrees of intrusiveness.” *Id.* at 737-38; *see also United States v. Quinzon*, 643 F.3d 1266, 1271-72 (9th Cir. 2011) (reviewing the breadth of various computer and Internet monitoring programs).

Here, Bislamian’s monitoring conditions are more tailored than those in *Sales*; Bislamian’s conditions list the particular devices to which they extend, and they do not extend to devices owned by any employer. Further, unlike in *Sales*, each condition could be related to the defendant’s crime and “the need for adequate deterrence.” *Bare*, 806 F.3d at 1020. Bislamian’s crime certainly involved computer use, and, unlike in *Sales*, the district court could properly infer that it involved Internet use.

In light of the deferential standard of review applicable to this case, we conclude that the district court did not plainly err by imposing the challenged search conditions.

AFFIRMED.