[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

FILED
U.S. COURT OF APPEALS
ELEVENTH CIRCUIT
DECEMBER 27, 2010
JOHN LEY
CLERK

No. 09-15265

D. C. Docket No. 09-60083-CR-WJZ

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

ROBERTO RODRIGUEZ,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of Florida

(December 27, 2010)

Before EDMONDSON, PRYOR and BARKSDALE,[*] Circuit Judges.

PRYOR, Circuit Judge:

---

[*] Honorable Rhesa H. Barksdale, United States Circuit Judge for the Fifth Circuit, sitting by designation.

The main issue in this appeal is whether the prying by a former bureaucrat is criminal: that is, whether the defendant violated the Computer Fraud and Abuse Act, which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). Roberto Rodriguez, a former employee of the Social Security Administration, appeals his conviction for violating the Act on the grounds that he did not exceed his authorized access to his former employer's databases and that he did not use the information to further another crime or to gain financially. The Administration prohibits accessing information on its databases for nonbusiness reasons, and Rodriguez at trial admitted that he accessed information for nonbusiness reasons when he obtained personal identifying information, such as birth dates and home addresses, of 17 persons he knew or their relatives. Rodriguez also appeals his sentence of 12 months of imprisonment on the ground that it is unreasonable. Because the record establishes that Rodriguez exceeded his authorized access and the Act does not require proof that Rodriguez used the information to further another crime or to gain financially, we **AFFIRM** his conviction. We also conclude that Rodriguez's sentence is reasonable.

I. BACKGROUND

From 1995 to 2009, Roberto Rodriguez worked as a TeleService representative for the Social Security Administration. Rodriguez's duties included answering questions of the general public about social security benefits over the telephone. As a part of his duties, Rodriguez had access to Administration databases that contained sensitive personal information, including any person's social security number, address, date of birth, father's name, mother's maiden name, amount and type of social security benefit received, and annual income.

The Administration established a policy that prohibits an employee from obtaining information from its databases without a business reason. The Administration informed its TeleService employees about its policy through mandatory training sessions, notices posted in the office, and a banner that appeared on every computer screen daily. The Administration also required TeleService employees annually to sign acknowledgment forms after receiving the policies in writing. The Administration warned employees that they faced criminal penalties if they violated policies on unauthorized use of databases. From 2006 to 2008, Rodriguez refused to sign the acknowledgment forms. He asked a supervisor rhetorically, "Why give the government rope to hang me?" To monitor access and prevent unauthorized use, the Administration issued unique personal

identification numbers and passwords to each TeleService employee and reviewed usage of the databases.

In August 2008, the Administration flagged Rodriguez's personal identification number for suspicious activity. Administration records established that Rodriguez had accessed the personal records of 17 different individuals for nonbusiness reasons. The Administration informed Rodriguez that it was conducting a criminal investigation into his use of the databases, but Rodriguez continued his unauthorized use. None of the 17 victims knew that Rodriguez had obtained their personal information without authorization until investigators informed them of his actions.

Most of Rodriguez's victims testified at trial. Cecilia Collins was married to Rodriguez from 1985 to 1990. In 2008 and 2009, Rodriguez used the Administration databases to determine how much Collins was earning. Rodriguez also accessed the personal information of Collins's sister for nonbusiness reasons.

Sally Culver lived with Rodriguez from 2001 to 2005. She testified that she had not spoken with Rodriguez since 2005. Culver testified that on one occasion, when she complained to Rodriguez about pay disparities at her place of work, Rodriguez stated that, if Culver gave him the name, birth date, and approximate age of a coworker, then he could tell her how much that coworker earned. Culver

declined Rodriguez's offer and did not provide him the coworker's name. Rodriguez also accessed the personal information of Culver's father for nonbusiness reasons. Rodriguez also told Culver that, if he was ever asked about his unauthorized searches, then he would make up an explanation. In 2008 and 2009, long after Culver and Rodriguez ended their relationship, Rodriguez accessed Culver's personal information 62 times.

Theresa Ivey had worked with Rodriguez at a post office, but Ivey had not spoken to Rodriguez since 1999. Ivey's daughter testified that she met Rodriguez in 1993 when she was a child. In 2008, Rodriguez accessed Ivey's personal information twice and her daughter's personal information 22 times.

Diamselis Rodriguez worked at a restaurant that Rodriguez frequently visited. Rodriguez gave Diamselis a pair of earrings on her birthday. In 2008, Rodriguez accessed Diamselis's personal information 20 times.

Dana Fennell, a professor of sociology from Mississippi, testified that she met Rodriguez at a Unitarian Universalist church study group when she was visiting her parents in Florida. Fennell interviewed Rodriguez for a study on the health effects of religion, but she did not consider him to be a friend. After Fennell returned to her home in Mississippi, she received flowers from Rodriguez on Valentine's Day even though she had not given Rodriguez her address. Rodriguez

later arrived at Fennell's doorstep unannounced, and Fennell was surprised and frightened by his presence. On another occasion, Rodriguez mentioned Fennell's father's birthday to Fennell even though she had never mentioned her father to Rodriguez. Rodriguez also told Fennell that he had the ability to listen to the telephone conversations of others. Rodriguez later called Fennell to wish her a happy "half-birthday" although she did not recall telling Rodriguez her date of birth. Rodriguez accessed Fennell's personal information on Administration databases 65 times, and he accessed the personal information of Fennell's mother and father multiple times.

Jessica Fox also met Rodriguez at the church study group. Fox testified that she received a letter from Rodriguez at her home address and was shocked because she had not given Rodriguez her address, she ordinarily receives all her mail at a post office box, and her middle initial was on the envelope although she had not used it since grade school. Rodriguez accessed Fox's personal information 45 times.

Rodriguez accessed the personal information of several other women he met at the church study group. Annemarie Jiovenetta considered Rodriguez to be an acquaintance, and Rodriguez accessed Jiovenetta's personal information 23 times. Joan Ginnell considered Rodriguez to be her friend, and she testified that he

seemed romantically interested in her. Rodriguez accessed Ginnell's personal information 30 times. Catherine Schuman avoided Rodriguez after it became apparent that he wanted a romantic relationship with her, and Rodriguez attempted to access her information 29 times. Rodriguez accessed Marianne Silverstein's personal information seven times and Jane Dekovitch's personal information ten times. Nitza Dominguez, did not testify at trial, but the government presented evidence that Rodriguez accessed Dominguez's personal information 34 times for nonbusiness reasons.

On April 2, 2009, a grand jury indicted Rodriguez with 17 misdemeanor counts of violating the Computer Fraud and Abuse Act. The indictment charged Rodriguez with "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). Trial commenced on July 27, 2009.

During opening statement, Rodriguez's attorney conceded that Rodriguez had "access[ed] things that were unauthorized." Rodriguez also testified in his defense and admitted accessing the personal information of the victims. Rodriguez testified that he had accessed the personal information as part of a whistle-blowing operation to test whether his unauthorized use of the databases would trigger the

attention of the Administration because he was conducting an investigation into improper denials of disability benefits. Rodriguez admitted that he did not access the victims' records as a part of his duties as a TeleService representative. On July 29, 2009, the jury rejected Rodriguez's argument about his conduct and returned a guilty verdict on all 17 counts.

The presentence investigation report provided a statutory maximum sentence of one year of imprisonment, 18 U.S.C. § 1030(c)(2)(A), and a sentencing guidelines range between zero and six months of imprisonment, United States Sentencing Guidelines § 2B1.1(a)(2) (Nov. 2008). Rodriguez did not object to the sentencing report. The government sought an upward variance from the guidelines range to 36 months of imprisonment. The government asked the district court to impose the statutory maximum of 12 months on some of the counts and order that the sentences run consecutively. The government argued that the guidelines range did not sufficiently account for the number of victims or the harm they suffered. The government also argued that an upward variance would better reflect the seriousness of the offense and promote respect for the law. At the sentencing hearing, Rodriguez presented more testimony about his discredited whistle-blowing motivation and expressed regret. Rodriguez requested a probationary sentence.

After considering the statutory factors for sentencing, 18 U.S.C. § 3553(a), the district court varied upward and sentenced Rodriguez to 12 months of imprisonment and 12 months of supervised release. The district court agreed with the government that the guidelines range did not adequately account for the number of Rodriguez's victims or the harm they suffered. Rodriguez objected to the upward variance.

II. STANDARDS OF REVIEW

Two standards of review apply in this appeal. We review questions of statutory interpretation de novo. United States v. Rahim, 431 F.3d 753, 756 (11th Cir. 2005). We review a sentence, "whether within or without the guidelines . . . only for reasonableness under an abuse of discretion standard." United States v. Irey, 612 F.3d 1160, 1186 (11th Cir. 2010) (en banc).

III. DISCUSSION

Our discussion of this appeal is divided in two parts. We first discuss whether Rodriguez's conduct supports a conviction under section 1030(a)(2)(B). Next, we discuss whether Rodriguez's sentence is reasonable.

A. Rodriguez Exceeded His Authorized Access Under Section 1030(a)(2)(B) When He Accessed Personal Records for Nonbusiness Reasons.

Rodriguez argues that he did not violate section 1030(a)(2)(B) because he accessed only databases that he was authorized to use as a TeleService

representative, but his argument ignores both the law and the record. The Computer Fraud and Abuse Act makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). The Act defines the phrase "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." Id. at § 1030(e)(6). The policy of the Administration is that use of databases to obtain personal information is authorized only when done for business reasons. Rodriguez conceded at trial that his access of the victims' personal information was not in furtherance of his duties as a TeleService representative and that "he did access things that were unauthorized." In the light of this record, the plain language of the Act forecloses any argument that Rodriguez did not exceed his authorized access.

Rodriguez contends that the interpretation of the Act by the Ninth Circuit in LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), supports his argument, but Rodriguez's reliance on Brekka is misplaced. The Ninth Circuit held that Brekka, an employee of a residential addiction treatment center, had not violated the Act when he emailed documents that he was authorized to obtain to his

personal email account. Id. at 1129. The treatment center argued that Brekka obtained the documents he emailed without authorization because he later used them for his own personal interests. Id. at 1132. The treatment center had no policy prohibiting employees from emailing company documents to personal email accounts, and there was no dispute that Brekka had been authorized to obtain the documents or to send the emails while he was employed. Id. at 1129. Brekka is distinguishable because the Administration told Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons.

Rodriguez also relies on United States v. John, 597 F.3d 263 (5th Cir. 2010), but his reliance on that decision too is misplaced. The Fifth Circuit held that use of information may constitute "exceeding authorized access," if the use is criminal. Id. at 271. John, an employee of Citigroup, was authorized to use her employer's computers and to view and print account information. Id. at 271. John used the information to incur fraudulent charges. Id. at 269. The Fifth Circuit observed that "John was authorized to view and print all of the information that she accessed," but concluded that "authorization" as used in the Act, "may encompass limits placed on the use of information obtained by permitted access to a computer system and data available on that system" if the use is in furtherance of a crime. Id. at 271–72 (internal quotation marks omitted). Rodriguez erroneously argues

that he cannot be convicted under the Act because his use of the information was not criminal. The problem with Rodriguez's argument is that his use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access. See § 1030(a)(2)(B). Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason.

Rodriguez also argues that his conviction cannot stand because he never used the personal information he accessed without authorization to defraud anyone or to gain financially, but this argument is foreclosed by the plain language of the Act. "The starting point for all statutory interpretation is the language of the statute itself[,]" and "we look to the entire statutory context." United States v. DBB, Inc., 180 F.3d 1277, 1281 (11th Cir. 1999). Sections 1030(c)(2)(B)(i) and (ii) of the Act provide a punishment of up to five years of imprisonment if "the offense was committed for purposes of commercial advantage or private financial gain [or if] the offense was committed in furtherance of any criminal or tortious act." 18 U.S.C. § 1030(c)(2)(B)(i), (ii). The misdemeanor penalty provision of the Act under which Rodriguez was convicted does not contain any language regarding purposes for committing the offense. See id. § 1030(c)(2)(A). Rodriguez's argument would eviscerate the distinction between these misdemeanor

and felony provisions. That Rodriguez did not use the information to defraud anyone or gain financially is irrelevant.

B. Rodriguez's Sentence is Reasonable.

Rodriguez argues that his sentence of 12 months of imprisonment is unreasonable both procedurally and substantively. The party challenging a sentence has the burden of establishing unreasonableness. United States v. Talley, 431 F.3d 784, 788 (11th Cir. 2005). To be upheld on appeal, a sentence must be both procedurally and substantively reasonable. United States v. Docampo, 573 F.3d 1091, 1100 (11th Cir. 2009). We consider each requirement in turn.

The district court committed no procedural error. A sentence is procedurally unreasonable if the district court erred by "failing to calculate (or improperly calculating) the Guidelines range, treating the Guidelines as mandatory, failing to consider the § 3553(a) factors, selecting a sentence based on clearly erroneous facts, or failing to adequately explain the chosen sentence—including an explanation for any deviation from the Guidelines range." Gall v. United States, 552 U.S. 38, 51, 128 S. Ct. 586, 597 (2007). The district court considered the guidelines range and the section 3553(a) factors and adequately explained Rodriguez's sentence.

Rodriguez argues that his sentence is procedurally unreasonable because the

district court should not have considered that there were multiple victims in its decision to vary upward because an enhancement under section 2B1.1(b)(2)(A) of the sentencing guidelines was the "proper mechanism" for considering multiple victims, but we disagree. This Court has held that a district court can rely on factors in imposing a variance that it had already considered in imposing an enhancement, United States v. Amedeo, 487 F.3d 823, 833–34 (11th Cir. 2007), and there is no requirement that a district court must impose an enhancement before granting a variance.

Rodriguez's burden of establishing that his sentence is substantively unreasonable is heavy. See Gall, 552 U.S. at 51, 128 S. Ct. at 597. The district court has wide discretion to decide whether the section 3553(a) factors justify a variance. See id. That we "might reasonably have concluded that a different sentence was appropriate is insufficient to justify reversal . . . ." Id. We will reverse only "if we are 'left with the definite and firm conviction that the district court committed a clear error of judgment in weighing the § 3553(a) factors by arriving at a sentence that lies outside the range of reasonable sentences dictated by the facts of the case.'" United States v. McBride, 511 F.3d 1293, 1297–98 (11th Cir. 2007) (quoting United States v. Williams, 456 F.3d 1353, 1363 (11th Cir. 2006)).

Rodriguez's sentence is substantively reasonable. Rodriguez argues that the sentence of 12 months of imprisonment is unreasonable because he is 54 years old, he has no prior criminal history, the offense was nonviolent, and he has already lost his job as a result of his actions, but the district court considered Rodriguez's personal characteristics and reasonably determined that an upward variance of six months was necessary to reflect the seriousness of the offense, promote respect for the law, and protect the public from future criminal conduct by Rodriguez. The district court was entitled to find that an upward variance was warranted based on the number of victims and the extensive nature of Rodriguez's unauthorized access. Although Rodriguez did not use the information he obtained to commit another crime, he used the information in a manner unwelcomed by his victims. Rodriguez's sentence of 12 months of imprisonment does not lie outside the range of reasonable sentences. See McBride, 511 F.3d at 1298. The district court did not abuse its discretion.

IV. CONCLUSION

The judgment of the district court is **AFFIRMED**.