628 F.3d 1258
United States Court of Appeals,
Eleventh Circuit.

UNITED STATES of America, Plaintiff–Appellee,
v.
Roberto RODRIGUEZ, Defendant–Appellant.

No. 09–15265. | Dec. 27, 2010.

* * *

PRYOR, Circuit Judge:

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 . . . .

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.

[The court details at length the women that Rodriguez accessed information about, including a former wife, a former long-term girlfriend, a waitress at a local restaurant, and church study group acquaintances.]

* * *

During his 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.

* * *

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) . . . .

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.* § 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.

* * *

IV. CONCLUSION

The judgment of the district court is AFFIRMED.