

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

MARK THOMAS ROSSINI,

Petitioner,

v.

Magistrate Case No. 08-692 (JMF)

UNITED STATES OF AMERICA,

Respondent.

MEMORANDUM OPINION

Currently pending and ready for resolution is the petitioner's Petition in Support of a Writ of Error *Coram Nobis* [#17]. For the reasons stated below, the petition will be denied.

BACKGROUND

On December 1, 2008, the government filed an information, claiming that on five occasions between January 19, 2007 and July 5, 2007, the petitioner "intentionally and knowingly exceeded his authorized access to a protected computer belonging to the Federal Bureau of Investigation, an agency of the United States headquartered in the District of Columbia, and by such act obtained information from the Federal Bureau of Investigation that he was not permitted to receive," in violation of Title 18 of the United States Code, Section 1030(a)(2)(B), the Computer Fraud and Abuse Act ("CFAA"). See Information [#1]. On December 8, 2008, the petitioner entered a guilty plea as to all charges in the information. See Plea Agreement (November 24, 2008 Letter from Tejpal S. Chawla, Assistant United States Attorney, to Adam Hoffinger, petitioner's counsel) [#3].

Pursuant to the plea agreement, the petitioner conceded that the following facts were true:

Between January 3, 2007 and July 30, 2007, the defendant made over 40 searches of the ACS for FBI information that were for purely personal purposes, and not connected to FBI business. Each of these searches exceeded the defendant's authorized use of the ACS system, and were [sic] not part of any of his assigned work. As part of these searches, the defendant obtained information to which he was not entitled.

Statement of the Offense [#4] at 3.

On May 14, 2009, the petitioner was sentenced to 1) twelve months of probation for each of the five counts, to run concurrently; 2) a special assessment fee of \$125; 3) a fine of \$5,000 to be paid at a monthly rate of \$250; and 4) 250 hours of community service. Judgment in a Criminal Case [#11] at 1, 3. Since judgment was imposed, the petitioner completed payment on the Court-imposed fines,¹ his supervised release was terminated,² and he completed his community service.³

DISCUSSION

I. Legal Standard

“The writ of *coram nobis* is an ancient common-law remedy designed ‘to correct errors of fact.’” U.S. v. Denedo, 556 U.S. 904, 910 (2009) (quoting U.S. v. Morgan, 346 U.S. 502, 507 (1954)). Originally, the writ was intended as a means of correcting “technical errors.” Denedo, 556 U.S. at 911. Today it is used to correct “fundamental errors,” when no other remedy is available. Id. Thus, “coram nobis . . . may collaterally

¹ See [#17-5] at 2

² See [#17-4] at 2.

³ See [#17] at 8.

attack only constitutional or jurisdictional errors or serious defects in the trial either not correctible on direct appeal or where exceptional circumstances justify the failure to appeal on those grounds.” U.S. v. McCord, 509 F.2d 334, 341 (D.C. Cir. 1974), cert. denied, 421 U.S. 930 (1975).

Writing in 2009, Judge Hogan indicated that “the D.C. Circuit’s precedent in this area is thin.” U.S. v. Williams, 630 F. Supp. 2d 28, 32 (D.D.C. 2009). He pointed to the leading case, United States v. Hansen, 906 F. Supp. 688 (D.D.C. 1990), in which Judge Joyce Hens Green of this Court, in the absence of D.C. Circuit authority for analyzing a petition for a writ of error *coram nobis*, looked to the practice of the Third, Fourth, Ninth and Tenth Circuits. Id. at 692. Under their precedents, relief by writ of *coram nobis* was only available when: “(1) a more usual remedy is not available; (2) valid reasons exist for not attacking the conviction earlier; (3) adverse consequences exist from the conviction sufficient to satisfy the case or controversy requirement of Article III; and (4) the error is of the most fundamental character.” Id. at 692-93. Accord U.S. v. Akinsade, 686 F.3d 248, 252 (4th Cir. 2012); Klein v. U.S., 880 F.2d 250, 254 (10th Cir. 1989); Hirabayashi v. U.S., 828 F.2d 591, 604 (9th Cir. 1987).

I will follow Judge Hogan’s and Judge Green’s lead and apply those factors.

II. Analysis

A. A More Usual Remedy is Not Available

Both the petitioner and the government agree that because the petitioner waived his right to an appeal when he accepted the plea agreement, and because he has now completed the various elements of his sentence, the more usual remedies of either a direct appeal or a motion for habeas corpus relief pursuant to 28 U.S.C. § 2255, respectively,

are not available. See [#17] at 13; United States['] Opposition to Defendant's Petition for Writ of Error Coram Nobis [#22] at 5. Thus, the petitioner has satisfied the first of the *coram nobis* requirements.

B. No Valid Reasons Exist for Not Attacking the Conviction Earlier

The petitioner argues that there was a valid reason why he did not attack his conviction earlier—because there was a change in the law governing his conviction. [#17] at 13-14. Specifically, the petitioner claims that it was not until this Court issued its decision in Lewis-Burke Assocs., LLC v. Widder, 725 F. Supp. 2d 187 (D.D.C. 2010) and the Ninth Circuit issued its decision in United States v. Nosal, 642 F.3d 781 (9th Cir. 2011), that he became aware that he had grounds to file a petition for a writ of *coram nobis*. [#17] at 17-18.

The government counters that the petitioner's argument is flawed because both the Widder and Nosal decisions adopted the Ninth Circuit's reasoning in LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), a decision issued in 2009, well before the petitioner's current filing, which occurred five years later on June 6, 2014. [#22] at 5-7. The government also argues that the petitioner could have based his argument on the reasoning in Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008), a 2008 decision in which the court ruled on the application of the CFAA to conduct similar to that at issue in this case. Id. at 6-7. The government's arguments are persuasive because there was authority in existence well before the petitioner filed his current petition, authority which could have supported the argument he makes now.

First, even if this Court's decision in Widder had been deemed to apply retroactively,⁴ which it was not, the petitioner still lacked a valid reason for not attacking his conviction earlier because the argument he now advances has in fact previously been successfully asserted, albeit not in this circuit. On February 20, 2008, the District Court for the District of Arizona issued its decision in Shamrock. In that case, a civil action,⁵ the court unequivocally held that "[t]he general purpose of the CFAA 'was to create a cause of action against computer hackers (e.g., electronic trespassers).'" Id. To that end, the court concluded the following with respect to sections 1030(a)(2)⁶ and section (4)⁷ of the CFAA:

Given the plain language, legislative history, and principles of statutory construction, the restrictive view of authorization is adopted. [A] violation for accessing without authorization occurs only where initial access is not permitted. And a violation for exceeding authorized access occurs where initial access is permitted but the access of certain information is not permitted.

Id. at 967 (internal citations and quotations omitted).

Less than two years later, on September 15, 2009, the Ninth Circuit issued its decision in Brekka. In that case, a company sued a former employee for violating sections 1030(a)(2) and (4) of the CFAA by accessing its computer *without* authorization and *in excess of* authorizations. Brekka, 581 F.3d at 1132. First, the court noted that "an

⁴ See U.S. v. Walgren, 885 F.2d 1417, 1421 (9th Cir. 1989) (holding that a decision deemed to have retroactive application generally also has such retroactive application in a *coram nobis* proceeding).

⁵ Although the CFAA is a criminal statute, it also provides for a civil cause of action between private parties. See 18 U.S.C. § 1030(g).

⁶ Section 1030(a)(2) states in pertinent part that a violation of the CFAA occurs when an individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information contained in a financial record . . . from any department or agency of the United States; or . . . from any protected computer."

⁷ Section 1030(a)(4) states in pertinent part that a violation of the CFAA occurs when an individual "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period."

employer gives an employee ‘authorization’ to access a company computer when the employer gives the employee permission to use it.” Id. at 1133. Thus, the court concluded that because the company gave the employee permission to access its computer, he did not act “without authorization” when he acted for purposes contrary to the company’s interest, both while employed by the company and then after he left the company. Id. at 1135. For the same reason, the court also concluded that the employee did not “exceed authorization.” Id. In a footnote, the court further noted that “nothing in the CFAA suggests that a defendant’s authorization to obtain information stored in a company computer is ‘exceeded’ [even] if the defendant breaches a state law duty of loyalty to an employer.” Id. at 1135 n.7. The court clearly stated therefore that an individual violates the above two sections of the CFAA by accessing data for which he lacks authorization, not for using data that he is authorized to access for purposes contrary to the company’s interest.

Finally, on July 28, 2010, this Court issued its decision in Widder. In that case, the issue before this Court was whether an employee violated the CFAA by taking confidential and proprietary computer data with him when he left the company where he used to work, in violation of section 1030(a)(2). As stated by the court in Shamrock, this Court also noted that the primary purpose of the CFAA was to deter computer hacking. Id. at 194. Then, following the Brekka line of cases, this Court noted that when an employer gives an employee permission to use its computer system, it is giving that employee authorization to access the data contained therein. Id. at 192. Ultimately, this Court concluded that “[w]hether [an employee] had permission to copy documents onto

his thumb drive or to subsequently use the data from a non-[work] computer, after he had left its employ, is not a question that relates to his liability under the CFAA.” Id. at 194.

As noted above, in this case, the information against the petitioner was filed on December 1, 2008, almost ten months after the February 20, 2008 Shamrock decision was issued. Understandably, even if the petitioner had been aware of the Shamrock opinion, he may not have felt compelled to base his motion for a writ of *coram nobis* upon the authority of a case from the District Court for the District of Arizona. However, when the Ninth Circuit issued its September 15, 2009 opinion in Brekka,⁸ the petitioner should have been compelled to file the current motion. In other words, as of the issuance of the Brekka decision, which was issued four months after the petitioner was sentenced, he should have been aware that there was circuit authority for the proposition that he was not guilty of a misdemeanor violation of the CFAA when he accessed FBI information for personal reasons.⁹ Nothing whatsoever justifies his delay.

C. The Petitioner Did Not Suffer Sufficient Adverse Consequences

First, the petitioner notes that “[t]he Supreme Court has recognized a presumption of collateral consequences that applies to a criminal conviction.” [#17] at 14 (citing Spencer v. Kemna, 523 U.S. 1, 9 (1998)). Then, the petitioner claims that, as a former FBI counterterrorism specialist who has been convicted of violating the CFAA, he has not been able to obtain work in his field of expertise. [#17] at 15.

⁸ Although the petitioner claims, *inter alia*, that it was not until the Ninth Circuit issued its decision in Nosal, that he became aware that he had grounds to file a petition for a writ of *coram nobis*, according to the court in Nosal, its conclusion “that an employer’s use restrictions define whether an employee ‘exceeds authorized access’ [was] simply an application of *Brekka*’s reasoning,” (Nosal, 642 F.3d at 787), and not a novel interpretation of the CFAA.

⁹ When new theories are advanced with respect to a law’s interpretation, even if those theories are not successful, the burden still lies with the petitioner to advance those theories in support of his case. See Durrani v. U.S., 294 F. Supp. 2d 204, 213 (D. Conn. 2003) (“The ‘availability of prior relief is determined by whether or not petitioner could attempt to secure such relief; it is irrelevant whether or not the petitioner would actually be successful in securing it.’”) (internal quotation omitted) aff’d 115 Fed. Appx. 500 (2004).

The government concedes that while it is true that adverse consequences flow from a criminal conviction, it argues that not every person who has been convicted of a crime is entitled to a writ of *coram nobis*. [#22] at 7. The government also notes the following: “His admitted behavior in conducting personal searches of the FBI database, obtaining information from that database, and sharing it with a third party would be an obvious impediment to any effort on his part to obtain future permanent employment in the counterterrorism field, quite separate and apart from the conviction to which that conduct lead.” *Id.* at 9.

Again, the government’s argument is persuasive. In order to satisfy the case or controversy requirement of Article III, the petitioner must show 1) that he suffered some actual or threatened injury as a result of the respondent’s conduct; 2) that the injury resulted from the petitioner’s conduct; and 3) that the injury is likely to be redressed by a favorable action. Valley Forge Christian Coll. v. Ams. United for Separation of Church and State, Inc., 454 U.S. 464, 472 (1982). In this case, even if the petitioner’s writ of *coram nobis* was granted and his conviction was vacated, the injury he claims he suffered—that he can no longer obtain employment in the field of counterterrorism—would not necessarily be redressed. In other words, the petitioner, of his own accord, admitted to having accessed information on the FBI database, over forty times, and used it for personal purposes. This behavior is hardly likely to make him an attractive candidate for future work in the field of counterterrorism, where the need to maintain secrecy is of paramount importance. In other words, had the petitioner not admitted to the conduct at issue, vacating his judgment would have favorably redressed his injury. Thus, the petitioner cannot be heard to argue that the adverse consequences he suffered

were either solely the result of his conviction or that they are sufficient to satisfy Article III's case or controversy requirement.

D. The Error is Not of the Most Fundamental Character

It is hard to understand what error of a fundamental character haunts the defendant's conviction. The defendant, represented by obviously competent counsel, chose to plead guilty and gain the benefits of doing so when he could have demanded a trial and asserted what might have been the successful argument that his behavior did not violate the statute. Instead, he chose to limit his sentencing exposure by pleading guilty. Now that the law is more favorable to his position, he wants to undo the bargain he made and get the result he chose not to try to get in the first place. A writ of *coram nobis* is designed to cure a fundamental error, not a bad case of buyer's remorse.

Alternatively, the defendant might argue that because the information did not charge a crime, this Court lacked jurisdiction over the subject matter and its exercising that jurisdiction to convict him was a fundamental error. See, e.g., U.S. v. Peters, 310 F.3d 709 (11th Cir. 2002). But, in this Circuit, it is clear that a claim that the indictment fails to state an offense does not deprive the court of jurisdiction over the subject matter. See U.S. v. Delgado-Garcia, 374 F.3d 1337, 1342 (D.C. Cir 2004). This is because the substantive sufficiency of the indictment is a matter that goes to the merits of the case, rather than to the district court's subject matter jurisdiction. Id. Accord U.S. v. George, 676 F.3d 249, 259-60 (1st Cir. 2012) (defendant pled guilty; so long as information charges a violation of a crime set out in Title 18 of the United States Code, that is the end of the inquiry as to subject matter jurisdiction). Thus, the only possible avenue of relief defendant could pursue is not available.

CONCLUSION

The defendant has failed to meet the criteria for *coram nobis* relief, other than the showing that the more usual remedies were not available to him. Thus, his motion will be denied.

An order accompanies this memorandum opinion.

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE