

1 RENE L. VALLADARES
Federal Public Defender
2 State Bar No. 11479
SHARI L. KAUFMAN
3 Assistant Federal Public Defender
411 E. Bonneville, Ste. 250
4 Las Vegas, Nevada 89101
(702) 388-6577
5 (Fax) 388-6261
6 Counsel for ANDRE NESTOR

7
8 UNITED STATES DISTRICT COURT
9 DISTRICT OF NEVADA
10

11 UNITED STATES OF AMERICA,
12 Plaintiff,
13 vs.
14 ANDRE NESTOR,
15 Defendant.

2:11-cr-00022-JCM-RJJ

**MOTION TO DISMISS COUNT THREE
OF THE INDICTMENT FOR FAILURE
TO STATE AN OFFENSE AND
VAGUENESS**
(Oral Argument Requested)

16
17 COMES NOW the defendant, ANDRE NESTOR, by and through his counsel of
18 record, Shari L. Kaufman, Assistant Federal Public Defender, and hereby moves this Court to enter
19 an order dismissing Count Three of the Indictment. This Motion is supported by the attached
20 Memorandum of Points and Authorities.
21

22 DATED this 9th day of November 2011.

23 RENE L. VALLADARES
24 Federal Public Defender

25 /s/ Shari L. Kaufman
26 By _____
SHARI L. KAUFMAN,
27 Assistant Federal Public Defender
28

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 **I.**

3 **STATEMENT OF FACTS**

4 On January 19, 2011, the United States Attorney for the District of Nevada filed a
5 three count indictment charging Andre Nestor (“Mr. Nestor”) and co-defendant John Kane (“Mr.
6 Kane”) with one count of Conspiracy to Commit Wire Fraud, a violation of 18 U.S.C. § 1349 (Count
7 One). (See Docket #12 (criminal indictment).) The government also charged Mr. Nestor with one
8 count of Fraud in Connection with Computers, a violation of 18 U.S.C. § 1030(a)(4) (Count Three).
9 Count Three alleges Mr. Nestor violated § 1030(a)(4) by knowingly and with the intent to defraud
10 access a protected computer in a manner that “exceed[ed] his authorized access.” The facts
11 pertaining to Count Three are as follows.

12 From on or about April 2009 to on or about September 2009, the government alleges
13 Mr. Nestor and Mr. Kane engaged in a conspiracy to obtain money by defrauding gaming machines
14 at casinos in Las Vegas, Nevada and Pennsylvania. The alleged fraudulent act involved exploiting
15 a programming glitch on certain multi-game video poker machines manufactured by International
16 Gaming Technologies, Inc. (IGT).

17 The government alleges Mr. Kane and Mr. Nestor illegally took advantage of the
18 glitch in the video poker machines in the following manner:

- 19 1. Mr. Kane and Mr. Nestor would ask an attendant to activate the “double up”
20 feature on certain IGT multi-game video poker machines.
- 21 2. After the attendant activated the “double up” feature, Mr. Kane and Mr.
22 Nestor would play a randomly selected game until they won a hand.
- 23 3. After winning a hand, they would then exit the game and select a different
24 poker game.
- 25 4. Again, they would play till they won another hand.
- 26 5. They would then insert either currency or a cash voucher into the machine.
- 27 6. They would then exit the game, and select a higher gambling denomination
28 (e.g., if they were originally playing \$1 per hand, they would switch to \$20)
- 29 7. They would then select the original game they played on the machine (see
30 step 2)

1 **A. Mr. Nestor’s Actions Do Not Constitute a Violation of the Computer Fraud and**
2 **Abuse Act Because: (1) the Gaming Machines Are Not “Protected Computers,”**
3 **and (2) Mr. Nestor Did Not “Access” or “Exceed his Authorized Access” to the**
4 **Machines.**

5 **1. 18 U.S.C. § 1030 – The Computer Fraud and Abuse Act**

6 Congress enacted the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, in
7 1984 to enhance the government’s ability to prosecute computer crimes. Initially, the act was
8 “designed to target hackers who accessed computers to steal information or to disrupt or destroy
9 computer functionality, as well as criminals who possessed the capacity to ‘access and control high
10 technology processes vital to our everyday lives....’” LVRC Holdings v. Brekka, 581 F.3d 1127,
11 1130-31 (9th Cir. 2009) (quoting H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 1984));
12 see also Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L.
13 Rev. 1561, 1563-64 (2010); Michael Hatcher, et al., Computer Crimes, 36 Am. Crim. L. Rev. 397,
14 402 (1999). Gradually, however, the CFAA has been expanded to encompass virtually any manner
15 of computer crime. The majority of crimes targeted by the CFAA involve accessing computers
16 without authorization or in excess of authorization, and then taking specific forbidden actions. See
17 18 U.S.C. § 1030(a)(1)–(7) (2008).

18 Pursuant to § 1030(a)(4), the statute at issue here, it is unlawful for a person to

19 knowingly and with intent to defraud, accesses a protected computer
20 without authorization, or exceeds authorized access, and by means of
21 such conduct furthers the intended fraud and obtains anything of
22 value, unless the object of the fraud and the thing obtained consists
23 only of the use of the computer and the value of such use is not more
24 than \$5,000 in any 1-year period.

25 18 U.S.C. § 1030(a)(4) (2008).

26 In order to obtain a conviction under § 1030(a)(4), the government must prove that
27 Mr. Nestor (1) accessed a “protected computer;” (2) exceeding authorization that was granted; (3)
28 knowingly and with intent to defraud and thereby; (4) furthered the intended fraud and obtained
anything of value; causing (5) “a loss to one or more persons during any one-year period aggregating
at least \$5,000 in value.” Brekka, 581 F.3d at 1133 (citing P.C. Yonkers, Inc. v. Celebrations the
Party and Seasonal Superstore LLC, 428 F.3d 504, 508 (3d. Cir. 2005) and Theofel v. Farley-Jones,
359 F.3d 1066, 1078 (9th Cir. 2004)). Only the first two elements—whether Mr. Nestor accessed

1 a “protected computer” in a manner that exceeded his authorized access—are relevant to the instant
2 motion.

3 **2. Mr. Nestor Did Not Access a “Protected Computer”**

4 Arguably, the gaming machines utilized in the alleged offense qualify as “computers”
5 under § 1030(e)(1). The CFAA defines a computer as

6 an electronic, magnetic, optical, electrochemical, or other high speed
7 data processing device performing logical, arithmetic, or storage
8 functions, and includes any data storage facility or communications
9 facility directly related or operating in conjunction with such device,
10 but such term does not include an automated typewriter or typesetter,
11 a portable hand held calculator, or other similar device.

12 18 U.S.C. § 1030(e)(1). According to IGT, the gaming machines it manufactures all contain a
13 processor board which regulates all game functions, including coin acceptance and delivery, game
14 statistical data accumulation and accounting, and player panel switches. See Introduction to Slots
15 and Video Gaming at 14.¹ Because the processor boards perform complex logical and storage
16 functions, the gaming machines are probably “computers” for the purposes of the CFAA. They are
17 not, however, “protected computers.”

18 In pertinent part, the CFAA defines a “protected computer” as a computer
19 which is used in or affecting interstate commerce or communication,
20 including a computer located outside the United States that is used in
21 a manner that affects interstate or foreign commerce or
22 communications of the United States.

23 18 U.S.C. § 1030(e)(2)(B).

24 The gaming machines here are not “protected computers” under this definition
25 because they are not “used in or affecting interstate commerce.” Courts which have addressed
26 whether a specific computer qualifies as a “protected computer” have uniformly agreed that a
27 connection to the internet is sufficient to establish a computer was used in interstate commerce and
28 is therefore a “protected computer.” See United States v. Fowler, 2010 WL 4269618 at *2 (M.D. Fla.
Oct. 25, 2010) (trial evidence that computers were connected to the internet sufficient to establish
use in interstate commerce); see also Multiven, Inc. v. Cisco Systems, Inc., 725 F.Supp. 2d 887, 891-

¹Available online at
<http://media.igt.com/Marketing/PromotionalLiterature/IntroductionTo Gaming.pdf>

1 92 (N.D.Cal. 2010) (finding that a computer connected to the internet was a protected computer);
2 National City Bank, N.A. v. Prime Lending, Inc., 2010 WL 2854247 at *4 n.2 (E.D.Wash. July 19,
3 2010) (stating that “any computer connected to the internet is a protected computer”); Expert
4 Janitorial, LLC v. Williams, 2010 WL 908740 at *8 (E.D.Tenn. Mar.12, 2010); Dedalus Foundation
5 v. Banach, 2009 WL 3398595, at *2 (S.D.N.Y. Oct.16, 2009) (unreported) (noting that courts have
6 “found that computers that access the Internet through programs such as email qualify as protected
7 computers”); Continental Group, Inc. v. KW Property Management, LLC, 622 F.Supp.2d 1357, 1370
8 (S.D.Fla.2009) (noting that a connection to the internet affects interstate commerce or
9 communication); United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (finding that computers
10 connected to the internet “were part of a system that is inexorably intertwined with interstate
11 commerce); accord United States v. Drew, 259 F.R.D. 449, 457-58 (C.D. Cal., 2009); U.S. v.
12 Walters, 182 Fed. Appx. 944, 945 (11th Cir.2006) (stating that the internet is an instrumentality of
13 interstate commerce).

14 Here, the government has produced no evidence the gaming machines accessed by
15 Mr. Nestor are connected to the internet or a network which uses interstate channels of
16 communications. Thus, at least under the above authority, the gaming machines do not appear to
17 be protected computers.

18 The CFAA is written broadly enough that it covers computers that are not connected
19 to the internet, so long as those computers are used to conduct business across state lines. See Patrick
20 Patterson Custom Homes, Inc. v. Bach, 586 F.Supp.2d 1026, 1033-34 (N.D.Ill.2008). (“[I]t suffices
21 to state the computer was used for the business and the business operated in two different states.”);
22 see also Kerr, supra, Vagueness Challenges at 1570-71 (noting that the CFAA applies to all
23 computers “so long as the federal government has the power to regulate them”). However, the
24 government has produced no evidence that the gaming machines are used in a manner which affects
25 interstate commerce. The gaming machines here were manufactured by a Nevada-based company,
26 are owned and operated by various Nevada-based gaming companies, and are regulated by a state
27 entity—the Nevada Gaming Control Board. Although this is probably a trial issue, there is no
28

1 indication that the strictly intrastate use and regulation of the gaming machines are used in interstate
2 commerce. Thus, they are not “protected computers” under the CFAA.

3 **3. Mr. Nestor Did Not Exceed His Authorized Access to the Gaming**
4 **Machines**

5 The government has also failed to demonstrate Mr. Nestor exceeded his authorized
6 access to the gaming machines in violation of the CFAA. As described above, the government
7 alleges Mr. Nestor violated § 1030(a)(4) by asking casino attendants to activate the “double up”
8 feature on certain models of IGT gaming machines, then performed a series of steps that exploited
9 a flaw in the machines’ programming to trigger a jackpot which paid out at a higher denomination
10 than Mr. Nestor had initially wagered. Although Mr. Nestor’s alleged actions may have violated
11 Nevada state law,² these actions did not exceed his authorized access to the gaming machine in
12 violation of the CFAA.

13 **a. The Various Definitions of “Access”**

14 The CFAA does not define “access.” Instead, it has been left to the courts to
15 determine what that word means in the context of the CFAA. This has resulted in a variety of
16 conclusions about what that term means. Under some definitions, a user only “accesses” a computer
17 when she is granted access “inside” the computer to manipulate information and processes. See
18 Orrin Kerr, Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse
19 Statutes, 78 N.Y.U. L. Rev. 1596, 1624-28 (2003) (citing State v. Allen, 917 P.2d 848 (Kan. 1996)
20 and Moulton v. VC3, 2000 WL 33310901 (N.D. Ga., 2000). Other courts have formulated broader
21 definitions, finding that “access” refers to mere physical “access” to a computer—for example,
22 sending an email to a computer. See id. at 1626-28 (comparing cases).³

23 ///

24 ///

25 ² See, e.g., Nev. Rev. Stat. § 465.070(3) (West 2011) (making it a crime to “claim,
26 collect or take...anything of value from a gambling game with the intent to defraud, without having
27 made a wager contingent thereon, or claim...an amount greater than the amount won”).

28 ³ As will be discussed below, the lack of consensus regarding the definition of
“access” supports Mr. Nestor’s assertion that § 1030 is unconstitutionally vague.

1 system displayed a notification which stated:

2 This computer system and information it stores and processes are the
3 property of Korn/Ferry. You need specific authority to access any
4 Korn/Ferry system or information and *to do so without the relevant
5 authority can lead to disciplinary action or criminal prosecution.*

6 Id. at 783 (emphasis in original). After Nosal left Korn/Ferry, he solicited three Korn/Ferry
7 employees to work for him. Id. Those three employees then obtained trade secrets by transferring
8 source lists, names, and contact information from Korn/Ferry’s database to Nosal. Id.

9 In finding that Nosal violated the CFAA, the Circuit formulated a broader
10 interpretation of “exceeds authorized access.” According to the Nosal panel, “the only logical
11 interpretation of ‘exceeds authorized access’ is that the employer has placed limitations on the
12 employee’s ‘permission to use’ the computer and the employee has violated—or ‘exceeded’—those
13 limitations.” Id. at 787. Unlike Brekka, the Nosal opinion seems to indicate that the mere act of
14 going beyond the scope of access as proscribed by an employer violates § 1030, regardless of
15 whether the employee exceeds her access for the purpose of obtaining information to which she is
16 not entitled. Thus, under the Nosal definition of “unauthorized access,” a violation of § 1030 might
17 occur under the following circumstances: a federal court employee, as part of her employment, is
18 required to use an office-issued computer to perform certain tasks like performing legal research.
19 If the employee uses that computer for some other purposes, such as visiting social networking sites
20 or checking her personal email account, that employee is potential committing a federal offense
21 under the CFAA.

22 **c. Mr. Nestor Did Not Violate the CFAA Under Either the Brekka or Nosal
23 Definition of “Exceeds Authorized Access”**

24 Regardless of which definition this Court chooses to apply, Mr. Nestor did not violate
25 § 1030(a)(4) by exceeding his authorized access to the gaming machine.⁵ As an initial matter, Mr.
26 Nestor did not “access” the gaming machine. As the government’s indictment alleges, Mr. Nestor
27 would ask a casino attendant to activate the “double up” feature on the gaming machines, and then

28 ⁵ As with the judicial conflicts regarding “access,” the tension between these two
definitions of “exceeds authorized access” support’s Mr. Nestor’s argument that § 1030 is
unconstitutionally vague.

1 would place wagers in a manner consistent with the machine’s user interface. There is no evidence
2 Mr. Nestor accessed or manipulated the information contained within the gaming machines’
3 processor—he was simply gambling in a way which was allowed by the machine.

4 Conceivably, Mr. Nestor might have “accessed” the computer if he had discovered
5 a way to manipulate the machines so that he was able to view information normally available only
6 to machine attendants or activate the “double up” feature, or used some external device to
7 manipulate the machines’ internal processes. The government has made no such allegation.
8 Moreover, it appears the only people who ever “accessed” the machines were the casino attendants
9 who activated the “double up” feature. Thus, the government has failed to allege Mr. Nestor
10 “accessed” the machines.

11 Even assuming Mr. Nestor “accessed” the machines, the government has failed to
12 allege Mr. Nestor “exceeded” his authorized access under either the Brekka or Nosal formulation
13 of the term. Applying the Brekka standard to the facts alleged by the government, Mr. Nestor did
14 not exceed his authorized access to the gaming machines because he did not “access information he
15 was not entitled to access.” Instead, as noted above, the casino attendants activated a special game
16 feature on the gaming machine, and Mr. Nestor played the games in a manner designed to ensure a
17 high payout. Knowing that a machine has a programming flaw, and pressing buttons in a manner
18 designed to exploit that flaw, is not equivalent to “accessing” information he was not entitled to
19 under Brekka.

20 The government’s allegations also fail to rise to the level of “exceeding authorized
21 access” under Nosal. Unlike Nosal, there is no evidence here that users of the gaming machines
22 were greeted with some sort of use disclaimer outlining the limitations on how they may use the
23 gaming machines when they sit down to play. More importantly, as noted repeatedly, the people in
24 control of the machines—the casino attendants—gave Mr. Nestor access to the “double up” feature.
25 Thus, any plays made during his granted access to the feature did not violate any limitations on his
26 play. Accordingly, Count Three of the indictment must be dismissed.

27 ///

28

1 **B. 18 U.S.C. § 1030 is Unconstitutionally Vague**

2 When construing a statute, a court ordinarily first looks to the plain meaning of the
3 language in question. See United States v. Hurt, 795 F.2d 765, 770 (9th Cir. 1986), as amended, 808
4 F.2d 707 (9th Cir. 1987). Given the competing definitions of “access” and “exceeds authorized
5 access” described above, § 1030 is unconstitutionally vague.

6 The vagueness doctrine “requires that a penal statute define the criminal offense with
7 sufficient definiteness that ordinary people can understand what conduct is prohibited and in a
8 manner that does not encourage arbitrary and discriminatory enforcement.” Kolender v. Lawson, 461
9 U.S. 352, 357 (1983) (internal citations omitted); see also Boyce Motor Lines v. United States, 342
10 U.S. 337, 340 (1952) (“A criminal statute must be sufficiently definite to give notice of the required
11 conduct to one who would avoid its penalties, and to guide the judge in its application and the lawyer
12 in defending one charged with its violation.”); Hoffman Estates v. Flipside, Hoffman Estates, Inc.,
13 455 U.S. 489, 498 (1982) (“[W]e insist that laws give the person of ordinary intelligence a
14 reasonable opportunity to know what is prohibited, so that he may act accordingly”).

15 A statute is unconstitutionally vague if it “fails to provide a person of ordinary
16 intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages
17 seriously discriminatory enforcement.” United States v. Williams, 553 U.S. 285, 304
18 (2008)(citations omitted); accord United States v. Kilbride, 584 F.3d 1240, 1257 (9th Cir. 2009).

19 The vagueness doctrine also reinforces fundamental notions concerning the control
20 of the discretion of law enforcement:

21 Although the doctrine focuses both on actual notice to citizens and
22 arbitrary enforcement, we have recognized recently that the more
23 important aspect of vagueness doctrine “is not actual notice, but the
24 other principal element of the doctrine—the requirement that a
25 legislature establish minimal guidelines to govern law enforcement.”

24 Kolender, 461 U.S. at 357-58 (citing Smith v. Goguen, 415 U.S. 566, 574 (1974)), accord City of
25 Chicago v. Morales, 527 U.S. 41, 60 (1999)(plurality).

26 “What renders a statute vague is not the possibility that it will sometimes be difficult
27 to determine whether the incriminating fact it establishes has been proved; but rather the
28 indeterminacy of precisely what the fact is.” Williams, 553 U.S. at 306 (citations omitted); accord

1 United States v. Schales, 546 F.3d 965, 973 (9th Cir. 2008). Here, the competing interpretations of
2 “access” and “exceeds authorized access” demonstrates there is indeterminacy regarding what acts
3 violate the statute.⁶

4 **III.**

5 **CONCLUSION**

6 Based upon the above and foregoing, Mr. Nestor respectfully requests this Court enter
7 an order dismissing Count Three of the Indictment.

8
9 Respectfully submitted:

10
11 /s/ Shari Kaufman

12 By: _____
13 SHARI L. KAUFMAN
14 Assistant Federal Public Defender

15
16
17
18
19
20
21
22
23
24
25
26 _____
27 ⁶ The Ninth Circuit may agree that the definition of “exceeds authorized access” has
28 not been satisfactorily addressed in either Brekka or Nosal. On October 27, 2011, the Circuit issued
an order that the case be reheard en banc. See United States v. Nosal, CA No. 10-10038 (9th Cir.
Oct. 27, 2011) (Order).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CERTIFICATE OF ELECTRONIC SERVICE

The undersigned hereby certifies that she is an employee of the Law Offices of the Federal Public Defender for the District of Nevada and is a person of such age and discretion as to be competent to serve papers.

That on November 9, 2011 she served an electronic copy of the above and foregoing **MOTION TO DISMISS COUNT THREE OF THE INDICTMENT FOR FAILURE TO STATE AN OFFENSE AND VAGUENESS (Oral Argument Requested)**, by electronic service (ECF) to the person named below:

DANIEL G. BOGDEN
United States Attorney
MICHAEL CHU
Assistant United States Attorney
333 Las Vegas Blvd. So., 5th Floor
Las Vegas, Nevada 89101

/s/ Bonnie S. Bell

Employee of the Federal Public Defender