FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. WILLIAM CARL SHEA, *Defendant-Appellant.*	No. 06-10450 D.C. No. CR-03-20057-RMW OPINION

Appeal from the United States District Court
for the Northern District of California
Ronald M. Whyte, District Judge, Presiding

Submitted May 14, 2007*
San Francisco, California

Filed July 11, 2007

Before: Cynthia Holcomb Hall, Diarmuid F. O'Scannlain, and Sandra S. Ikuta, Circuit Judges.

Opinion by Judge Hall

*This panel unanimously finds this case suitable for decision without oral argument. *See* Fed. R. App. P. 34(a)(2).

COUNSEL

Arthur Pirelli, San Rafael, California, for the appellant.

Amber S. Rosen, Assistant United States Attorney, San Jose, California, for the appellee.

OPINION

HALL, Senior Circuit Judge:

Defendant William Carl Shea challenges his conviction for intentionally causing damage to a "protected computer" without authorization, in violation of 18 U.S.C. § 1030(a)(5)(A)(i). Shea argues that the government presented insufficient evidence to convict, and, more specifically, presented no evidence that he committed a criminal act on the date alleged in the indictment. He also argues that the district court improperly denied his request for substitute counsel. We disagree with each of Shea's contentions and, therefore, affirm the conviction.

I. Background

The defendant was an employee at Bay Area Credit Services (BACS) from August 6, 2001, until January 17, 2003. BACS provides debt collection services, and Shea managed the company's database operating system, which was designed by a company called Columbia Ultimate. In December 2002, Shea asked for permission to work from home because his daughter had been diagnosed with diabetes, but his request was denied because, as BACS CEO Michael Priest testified, Shea had been unproductive and difficult to reach during his previous stints working at home.

On January 6, 2003, company executives met with Shea and gave him a "performance plan" requiring him to meet cer-

tain productivity targets and to communicate with his superiors about any planned absences. Shea did not come in to work on January 17 and was subsequently terminated.

On January 30, BACS discovered that its database of debtor accounts had been corrupted. It discovered a foreign program on its system that was coded to replace debt principal amounts with random numbers, switch client identification numbers and eliminate the Social Security numbers tied to each account. The program was coded to modify 5,000 records at a time and to repeat after each batch. Later investigation revealed that the program had stopped on its own because it had run multiple, simultaneous sessions. Before the program "hung," however, it had corrupted approximately 50,000 entries. BACS and representatives from Columbia Ultimate, who had designed its database software, were able to retrieve much of the data, but the process took approximately two months to resolve and cost BACS thousands of dollars in fees to technical support consultants.

BACS and Columbia Ultimate blamed the file corruption on a program called "CLEAR.CF.MARKS," which used a file naming convention similar to other files on the BACS system. For example, there was a CLEAR-CF-MARKS in the same file directory. CLEAR.CF.MARKS was triggered by one line of code in the program "Collector-Summary-II," which was an authorized program that ran late in the evening or early in morning to process the previous day's collection activities, as logged by BACS debt collectors.

Government witnesses estimated that CLEAR.CF.MARKS had been on the BACS system since at least December 9, 2002. They made this estimation based on the fact that on December 9, the relevant line of Collector-Summary-II's code had been edited to launch CLEAR.CF.MARKS. Back-up tapes indicated that the program had not been on the system in September 2002.

The government referred to CLEAR.CF.MARKS as a "time bomb" program. Though Collector-Summary-II presumably launched the program every night since December 9, CLEAR.CF.MARKS would not actually detonate, continuing the government's metaphor, until a date provided in its own source code. Though CLEAR.CF.MARKS deleted its own source code as part of its operation, back-up tapes revealed a copy of the source code that set the trigger date at any date "greater than" January 29, 2003.

Columbia Ultimate consultants assisting BACS looked through hard drive back-up materials and network logs to investigate the origins of the malicious program. They discovered that a person using various log-in names and passwords associated with Shea had made edits to both Collector-Summary-II and the source code for CLEAR.CF.MARKS during December 2002 and January 2003. Shea had been hired specifically in 2002 to help BACS convert to the latest release of Columbia Ultimate's software and remained on staff as its programmer. He had experience in many programming languages including those necessary to access the IBM "Universe" databases Columbia Ultimate designed for BACS and to work in the code of the files it contained. In his previous jobs, Shea worked with several of the Columbia Ultimate employees who were called in to fix the problem on January 30.

FBI Agent Andrew Myers interviewed Shea at his home on March 28, 2003. When Agent Myers presented Shea with a copy of the source code of CLEAR.CF.MARKS, Shea immediately recognized the program as foreign to the system, and remarked that it should have been titled CLEAR-CF-MARKS, with dashes instead of dots. Upon a brief examination of the code, Shea noted that it would likely cause debt amounts to be altered. He said he thought the program would not run and would eventually "hang itself."

When the agents pointed out that his user name had been associated with the file, Shea initially denied authoring the

program and offered no hypothesis as to why his user name was involved. Upon further questioning he stated that at the time the code was written he was experiencing medical problems. According to the agent, Shea also said that he had "difficulty determining if events were real or if he was dreaming them." Shea also explained his problems with BACS, and that he thought people at the company were "out to get him."

The initial indictment charging Shea was returned on April 30, 2003, and was superseded by a new indictment on August 5, 2004. A Second Superceding Indictment was returned on August 3, 2005, charging Shea with seven counts of intentionally causing damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A)(i). Each count corresponded to a particular act of entering or editing code on seven different dates before the program corrupted the database.

During his trial, at the close of evidence, Shea moved for appointment of new counsel. The court denied this request. Shea moved for dismissal of six of the seven counts, and moved for dismissal on the remaining count under Rule 29 of the Federal Rules of Criminal Procedure. After consulting with the parties, the district court consolidated the counts into count 7, which related to January 29, 2003. It did not expressly rule on Shea's motion to dismiss the remaining count.

The jury convicted Shea, and the district court sentenced him to twelve months and one day in prison. He was also ordered to pay $40,000 in restitution. This timely appeal followed.

II. Sufficiency of the Evidence

"There is sufficient evidence to support a conviction if, viewing the evidence in the light most favorable to the prosecution and drawing all reasonable inferences, any rational trier of fact could have found the essential elements of the

crime beyond a reasonable doubt." *United States v. Bazuaye*, 240 F.3d 861, 863 (9th Cir. 2001); *see also Jackson v. Virginia*, 443 U.S. 307, 319 (1979). "Circumstantial evidence and inferences drawn from it may be sufficient to sustain a conviction." *United States v. Jackson*, 72 F.3d 1370, 1381 (9th Cir. 1995). When the issue of sufficiency of the evidence is preserved by making a motion for acquittal, we review the district court's denial of the motion de novo. *United States v. Tucker*, 133 F.3d 1208, 1214 (9th Cir. 1998).

[1] We have had rare occasion to interpret sufficiency of the evidence under the Computer Fraud and Abuse Act, which punishes any person who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A)(i). Our decisions have thus far concentrated on the issue of damages. *See, e.g.*, *United States v. Middleton*, 231 F.3d 1207 (9th Cir. 2000); *United States v. Sablan*, 92 F.3d 865 (9th Cir. 1996). Damages are not at issue in this appeal — only the question of the defendant's involvement. Our analysis here is therefore aided by applicable principles from decisions interpreting similar criminal statutes.

[2] Wire fraud, like computer fraud, has transmission as one of its elements. *See* 18 U.S.C. § 1343. To prosecute crimes involving the element of "transmission," the government must offer sufficient proof that the person charged is the same person who sent the transmission. Circumstantial evidence is sufficient to prove that the transmission has occurred. *See United States v. Rush*, 749 F.2d 1369, 1373 (9th Cir. 1984). We confronted a wire fraud conviction based on facts similar to those presented here in *United States v. Mullins*, 992 F.2d 1472 (9th Cir. 1993). In that case, a trio of travel agents had manipulated an airline's reservation system to transfer frequent flyer miles into sham accounts. *Id.* at 1475. The government witness testified that each of these transfers was tied to one of the defendants' passwords, and an FBI

search of their offices revealed records of the ticket sales tied to their fake accounts. *Id*. The defendants argued, as Shea does in this case, that other employees could have accessed the passwords and accounts, and that the system was generally not secure. *Id.* at 1477. Nevertheless, we observed that there was "overwhelming" evidence to support the conviction, despite the possibility that someone else accessed the computer. *Id.*

We have also found analogous cases where computer transmissions provided the basis for the prosecution's theory, even if "transmission" itself was not an element of the offense. In our review of a bank fraud prosecution, we found sufficient evidence to support a conviction where the defendant had deployed a computer program to alter ATM records. *See United States v. Bonallo*, 858 F.2d 1427 (9th Cir. 1988). We noted that the defendant had the necessary programming skills, and the program file was found in his own file library. *Id.* at 1434. Because the government had also offered evidence of the defendant's comings and goings from the banks in question, the sufficiency ruling did not rest on access and programming skills alone. *Id.*

In an Eighth Circuit case bearing some resemblance to Shea's, the court found sufficient evidence to support an extortion conviction where the defendant argued he had not sent the e-mails at issue. *See United States v. Ray*, 428 F.3d 1172, 1174 (8th Cir. 2005) (per curiam). A computer expert had testified that the e-mails were created on the defendant's computer and saved on that computer's hard drive. *Id.* The e-mails had been sent at a time when the defendant was using his computer, and there was no evidence of remote access to the computer at the time. *Id.* The evidence also showed the defendant had the knowledge and ability to follow through on the threats presented in the emails. *Id*. In another Eighth Circuit case, the court upheld an aiding and abetting conviction where there was no direct evidence that the defendant had used the computer where files had been improperly down-

loaded. *See United States v. Levine*, 477 F.3d 596, 605-06 (8th Cir. 2007). The court held that the evidence offered, proving the defendant's access to the computer and the defendant's motive, was sufficient. *Id.*

At Shea's trial, the prosecution constructed a timeline for the two relevant programs: Collector-Summary-II, the authorized program used in the day-end process, and CLEAR.CF.MARKS, the "time bomb," which was launched by Collector-Summary-II. Both the prosecution and the defense elicited a great deal of testimony on how the BACS computer system works. For our purposes, it is relevant to describe the multiple levels of network and database access available to BACS employees:

(1) BACS employees signed in to a Windows network where each employee had a user name and could select a personal password;

(2) from there, they could log on to the database of the Columbia Ultimate Business System (CUBS), which operated on a Unix platform, as opposed to Windows. To work on the database, BACS employees had individual user names (which were also tied to user numbers) and selected their own passwords;

(3) certain employees could also sign in to the Collector System, through distinct passwords that were assigned to each of them and based on their Social Security numbers. These passwords were archived in a separate file readable by only certain higher-level employees.

These user names and passwords were not tied to each other, or to any given machine. So, for example, a person who knew all the relevant names and passwords could log in as one employee for the BACS Windows network, and then log in as another employee for the CUBS Universe database, and then sign in to the Collector System using another employee's

password. The defense highlighted that any user could switch Unix identities in the CUBS database (the second level) with the right passwords, and that certain employees had "root" access or "super user" access that gave them permission to access any part of the system, though a password would still be necessary to enter the Collector System. Shea had root and super user access and could also access the list of employee passwords for the Collector System.

The following timeline could be constructed from the testimony at trial:

On December 9, 2002, at 6:53 p.m., a person logged on to the BACS network using Shea's Windows user name at a computer in Shea's office. A person at the same time logged on to the CUBS database under the Unix user name assigned to "LIB2002." This account had been created during the system conversion to the latest release of CUBS — the job for which Shea was initially hired. This Unix user accessed the Collector-Summary-II source code and edited one line of the code to execute CLEAR.CF.MARKS.

On December 27, 2002, at 10 a.m., BACS CEO Michael Priest called Shea into his office to discuss his work habits, which were "below acceptable," according to Shea's supervisor. At 2:23 p.m. that day, the Collector System logs indicated that user SHEAB edited the source code of CLEAR.CF.MARKS to change the trigger date from January 22 to January 15, 2003.[1]

[1]There are two types of code involved in this case. "Source code" is essentially a set of directions that a programmer writes in text form. When the source code is complete, the programmer runs the code through a "compiler" that produces "object code" in a language that only the computer can read. *See Microsoft Corp. v. AT&T Corp.*, 127 S. Ct. 1746, 1754 n.8 (April 30, 2007) ("Software in the form in which it is written and understood by humans is called source code. To be functional, however, software must be converted (or compiled) into its machine-useable ver-

On January 6, 2003, Shea's supervisor, CIO William Stambaugh informed Shea that he would have to submit to a "performance plan," which dictated that he check in by phone when he planned to be absent. The next day, January 7, at 7:27 a.m., Unix user 412, an identity tied to Shea, compiled the source code of CLEAR.CF.MARKS into object code. This date and time is the last recorded access to the CLEAR.CF.MARKS object code. Therefore, further alterations to the source code would not have affected the program that eventually ran on January 29.[2]

On January 9, at 11:36 a.m., user SHEAB accessed the source code, but BACS's logs do not show that any modifications were made. The logs also show that the user entered a code to delete any record of commands entered by SHEAB. This user also entered a "clear screen" command several times, to move all text off the screen. Clearing the screen would have prevented anyone from observing the commands that were being typed. This user also entered a "WHO" command to confirm which user identity would be tied to the commands in the company's logs.

On January 15, CLEAR.CF.MARKS would have run based on the source code changes made in December, but it did not

---

sion, a sequence of binary number instructions typed object code." (internal citation and quotations omitted)). *See also Blueport Co., LLP v. United States*, 02-1622 C, ___ Fed.Cl. ___, 2007 WL 1321740 at *31 n.11 (Fed. Cl. May 7, 2007).

The government witnesses analogized this distinction in two ways: First, the source code as the recipe for a pie, and the object code as the actual pie. Second, the source code can be seen as the design for an assembly line, and the object code as the assembly line itself. On the BACS system, source code was stored in one file directory, and object code was stored in another. This distinction helped BACS and Columbia Ultimate determine which file had been edited by looking at the directory marker.

[2]The pie was baking in the oven, to continue the metaphor. Alternatively, the time bomb fuse had been lit, in the government's phrasing.

— suggesting changes to the date had been made at some other time prior to January 7, when the source code was compiled into object code. The government offered evidence that the final source code had a trigger date of January 29. This date was written in a computer programming language called "Pick," which Shea, but few others in the company, knew.

On January 16, "SHEAB" again accessed the program but the log reflected no modification. The next day, a Friday, Shea did not show up for work, and Stambaugh decided to terminate him. Shea was apprised of his termination at the office on Monday, January 20. CLEAR.CF.MARKS allegedly triggered early in the morning January 30.

[3] Viewing the evidence in the light most favorable to the prosecution, with all reasonable inferences that can be drawn from the record, we hold that a rational juror could have found Shea guilty. His access to the relevant files is undisputed. His ability to program in the Unix database and in the Collector System files is undisputed and appears to have been unique among BACS employees. His antagonistic relationship with BACS executives provided him with a motive, and the timing of certain edits corresponds with the meetings and e-mails that preceded his termination.

Shea argues that there is no evidence that he compiled the source code a second time, after January 7, to change the trigger date from January 15 to January 29. The government, however, offered evidence that the final version of the source code did contain the date of January 29. Drawing reasonable inferences from the record, this edit must have occurred before January 7, otherwise the "time bomb" would have gone off on January 15, and it did not. Though the government did not offer any evidence of this second change, the circumstantial evidence that the change occurred is sufficient to sustain the conviction on appeal.

[4] Shea also argues that several other BACS employees had access to his computer or could have logged on as him

remotely. He presented evidence to the jury that another BACS employee was logged in from Shea's desktop computer at all the relevant times. However, given Shea's level of access, which included access to the Unix names and passwords of all other BACS employees, and given Shea's tendency to open multiple sessions at once from his computer, operating from both his laptop and desktop computers, a juror could reasonably infer that Shea had logged in as the other employee during all the relevant times. Because the prosecution "need not affirmatively rule out every hypothesis except that of guilt," *Wright v. West*, 505 U.S. 277, 296 (1992) (internal quotation marks omitted), we find that reasonable inferences from this record support Shea's conviction.

III. Variance Between Indictment and Evidence

Shea makes a more specific sufficiency claim that he committed no act on January 29, the date identified in the sole count of the final indictment. Shea argues that the only provable act — compiling the code on January 7 — constituted mere preparation that was not directly tied to the ultimate damage caused by CLEAR.CF.MARKS. We find these arguments unpersuasive.

[5] Neither the language of the indictment, nor 18 U.S.C. § 1030(a)(5)(A)(i), required the government to prove that Shea committed any act on January 29. Section 1030(a)(5)(A)(i) requires proof that a defendant "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." The government's proof that Shea knowingly added instructions to the company's programs at some date in January to cause the CLEAR.CF.MARKS routine to run on or about January 29, 2003, was sufficient. Accordingly, we hold that there was no variance between the indictment and evidence adduced at trial.

Moreover, even if Shea could establish a variance between the charges set forth in his indictment and the evidence adduced at trial, we would reach the same result. Where, as here, the date is not a material element of the offense, any variance between the date charged in the indictment and proof of the date at trial is harmless error if it does not affect the defendant's substantial rights. *See United States v. Tsinhnahijinnie*, 112 F.3d 988, 991 (9th Cir. 1997). Specifically, the variance must not be " 'of a character which could have misled the defendant at the trial' " and must not present a danger of double jeopardy. *Id.* (quoting *Berger v. United States*, 295 U.S. 78, 83 (1935)).

A variance typically is immaterial if the government has proven that the criminal act occurred on a date "reasonably near" the date cited in the indictment. *See United States v. Hinton*, 222 F.3d 664, 672-73 (9th Cir. 2000) (eighteen days); *United States v. Baker*, 10 F.3d 1374, 1419 (9th Cir. 1993) (two months), *overruled on other grounds by United States v. Nordby*, 225 F.3d 1053 (9th Cir. 2000); *Lelles v. United States*, 241 F.2d 21, 25 (9th Cir. 1957) (nineteen days). *But see Tsinhnahijinnie*, 112 F.3d at 991 (two years); *United States v. Casterline*, 103 F.3d 76, 78-79 (9th Cir. 1996) (seven months).

[6] Here, the prosecution offered proof of the defendant's actions on six dates between December 9, 2002, and January 16, 2003, with the final damage occurring on January 29, 2003. Because he went to trial assuming seven counts relating to each of those dates, Shea was clearly not prejudiced by the consolidation into one count relating to one date. The indictment, despite its many amendments, "sufficiently notif[ied] the defendant of the charges against him and enable[d] him to prepare a defense." *United States v. Laykin*, 886 F.2d 1534, 1542 (9th Cir. 1989). Therefore, we reject Shea's argument based on this discrepancy.

IV. Request for New Counsel

Shea argues he was entitled to new counsel because his trial counsel failed to elicit certain testimony about his programming skills, the possibility that other people may have figured out how to program in the required languages, and his ability to delete all the records if he had wanted to. When the district court denied Shea's request, it observed that many of his points had been brought out on cross examination, that trial counsel was entitled to make strategy decisions, and that Shea appeared to get along with this attorney. We review this decision for abuse of discretion. *United States v. George*, 85 F.3d 1433, 1438 (9th Cir. 1996).

[7] Our review considers three factors: (1) the timeliness of the motion; (2) the adequacy of the court's inquiry into the defendant's complaint; and (3) whether the conflict between the defendant and his attorney was so great that it resulted in a total lack of communication preventing an adequate legal defense. *Id.*

[8] Applying these factors, we find that little weighs in Shea's favor. He made this motion midtrial, was granted considerable time to explain his problems with his counsel, and clearly had discussed these issues with his attorney. *See id*. His counsel's decision not to present a defense was tactical and within her discretion. *See United States v. Appoloney*, 761 F.2d 520, 525 (9th Cir. 1985). Therefore, we hold that the district court did not abuse its discretion in denying Shea's motion.

V. Conclusion

We hold that the evidence was sufficient to support Shea's conviction, that any variance between the date in the indictment and the date of Shea's acts was immaterial, and that the district court's refusal to appoint new counsel was appropri-

ate. Therefore, the conviction is

AFFIRMED.