

52 Va. Cir. 156, *; 2000 Va. Cir. LEXIS 246, **

Commonwealth of Virginia v. Jon Michael **Honhart**

Case No. (Criminal) 96656

CIRCUIT COURT OF FAIRFAX COUNTY, VIRGINIA

52 Va. Cir. 156; 2000 Va. Cir. LEXIS 246

April 14, 2000, Decided

CASE SUMMARY

PROCEDURAL POSTURE: Defendant entered a plea of not guilty to the Commonwealth's indictment charging computer trespass. After deliberation, the jury found the defendant guilty of a lesser-included misdemeanor. Defendant renewed his motion to strike the indictment, and defendant moved the court to set aside the verdict and dismiss the charge or, in the alternative, to order a new trial.

OVERVIEW: Defendant was employed as a systems engineer, but he left for employment with another company at an increased salary. Defendant's former employer experienced severe server and network problems. A police detective testified that the defendant accessed kernel files. The detective could not tell what the defendant did to the kernel files. Va. Code Ann. § 18.2-152.4(A)(2) provided that it was unlawful for any person to use a computer or computer network without authority and with the intent to cause a computer to malfunction regardless of how long the malfunction persisted. The Commonwealth's burden was to prove that defendant did more than simply halt another's computer; the evidence had to establish beyond a reasonable doubt that defendant intended his actions to cause a malfunction of another's machine. The jury could conclude that the Commonwealth linked defendant's computer activities to the computer shut down at his former employer and that there was an inability of the system to re-boot after the shutdown. However, no direct evidence established that the computer malfunction resulted from the defendant's or anyone's deliberate act.

OUTCOME: Defendant's motion to strike was granted and the indictment dismissed. The evidence did not exclude the reasonable hypothesis of innocence that defendant accidentally adversely effected the kernel. Under controlling authority, the evidence supported a reasonable hypothesis of innocence.

CORE TERMS: network, kernel, malfunction, shut down, firewall, log, business records, custodian, evidence presented, hypothesis, attendance, innocence, operating system, administrator, accessed, halting, server, reasonable doubt, indictment, direct evidence, intent to cause, certificate, circumstantial, accidentally, repercussions, webserver, re-boot, machine, message, logged

LexisNexis(R) Headnotes ♦ [Hide Headnotes](#)

[Criminal Law & Procedure](#) > [Appeals](#) > [Standards of Review](#) > [Standards Generally](#) 

HN1 ↓

When a defendant challenges the sufficiency of the evidence, an appellate court must give full faith and credit to the witnesses and draw all inferences from their testimony that a jury might fairly draw therefrom. [More Like This Headnote](#)

[Criminal Law & Procedure](#) > [Trials](#) > [Burdens of Proof](#) > [Prosecution](#) 

HN2 ↓

The Commonwealth always bears the burden of proving guilt beyond a reasonable doubt. When the Commonwealth relies solely upon circumstantial evidence to identify a criminal agent, it bears the burden of excluding every reasonable hypothesis of innocence, that is, those which flow from the evidence itself, and not from the imagination of defendant's counsel. [More Like This Headnote](#)

♦ [Show Headnotes / Syllabus](#)

JUDGES: **[**1]** BY JUDGE R. TERRENCE NEY

OPINIONBY: Ney

OPINION: **[*156]**

This matter comes before the Court on the Defendant's Motion for Certificate for Out of State Witness.

The Court has considered the arguments of counsel and reviewed the eight documents produced by Microsoft Corporation and submitted to the Court at hearing ("the Microsoft documents"). Without holding that the Microsoft documents are business records, the Court considers it extremely likely that the Defendant will be able to have these documents admitted into evidence as business records at trial based upon the testimony of a Microsoft custodian of records who can testify that they were made and kept in the ordinary course of business, that they were made contemporaneously with the events described, and that they were made by persons having a duty to keep a true record. See Sparks v. Commonwealth, 24 Va. App. 279, 482 S.E.2d 69 (1997). Therefore, the court finds that the custodian of these records from Microsoft Corporation is a material witness and will issue a certificate under the seal of the Court, pursuant to Va. Code § 19.2-277, so that Defendant's counsel may obtain an order from a Washington State court to compel the attendance **[**2]** of the proper Microsoft custodian.

Because the need for the Microsoft custodian's attendance at trial is occasioned by the Commonwealth's refusal to stipulate that the Microsoft documents are business records, yet the Assistant Commonwealth's Attorney is unable to proffer to the Court

any reason why they are not business records [*157] as set forth in Sparks, the Court will require the Commonwealth to pay for the attendance of the Microsoft witness at trial pursuant to Va. Code § 19.2-278.

July 27, 2000

BY JUDGE DENNIS J. SMITH

Smith

On May 1, 2000, the Defendant, Jon Michael **Honhart**, appeared before this court with his counsel, W. Steven Paleos and Brian Cabbage, and entered a plea of not guilty to the Commonwealth's indictment n1 charging Computer Trespass, a felony under § 18.2-152.4 of the Virginia Code. The Defendant moved to strike the evidence presented at the conclusion of the Commonwealth's case and then again after all the evidence was presented. The court denied the defendant's Motion to Strike the Evidence when made at the conclusion of the Commonwealth's case, but when the Motion was renewed at the conclusion of all evidence, the court took the matter under **[**3]** advisement. Closing arguments were heard on May 4, 2000, and the jury received instructions. After deliberation, the jury found the Defendant guilty of the lesser-included misdemeanor violation under the same code section. In addition to his Motion to Strike, the Defendant now moves the court to set aside the verdict and dismiss the charge or, in the alternative, to order a new trial.

----- Footnotes -----

n1 The Court read Mr. **Honhart** the charge as follows, "[O]n or about the 20th of April, 1999, in the County of Fairfax, you, Jon M. **Honhart**, used a computer or computer network without authority and with the intent to cause a computer to malfunction and that such act was done maliciously, causing damage to property of another in excess of twenty-five hundred dollars, in violation of Virginia Code § 18.2-52.4." Record at 70.

----- End Footnotes -----

Whether the Court is considering a Motion to Strike the Evidence at the conclusion of the trial or a Motion to Set Aside the Verdict made after the trial which is based upon insufficiency of the evidence, the **[**4]** standard of review is the same. See Rule 3A:15 of the Rules of the Virginia Supreme Court. ^{HNI}When a defendant challenges the sufficiency of the evidence, the court must "giv[e] full faith and credit to the witnesses and [draw] all inferences from their testimony that a jury might fairly [draw] therefrom." Limbaugh v. Commonwealth, 149 Va. 383, 393, 140 S.E. 133 (1927); see also Tyler v. Commonwealth, 254 Va. 162, 165, 487 S.E.2d 221 (1997).

When viewed in this light, the evidence presented established that The Signature Group (TSG) is a computer consulting company, which employed Mr. **Honhart** as a Systems Engineer from October 5, 1998, until April 15, **[*158]** 1999, at which time he left for employment with another company at an increased salary. On April 21, 1999, TSG experienced severe server and network problems; in lay terms, TSG's network "crashed." Scott Lucier, an administrator and the program manager at TSG, discovered the system's crash and noted an error message on the computer network

and the webserver stating that there was an error in the "kernel." See Record at 110. Neither the network nor the webserver would "re-boot." Mr. Lucier reviewed the firewall log n2 and noted [**5] that on April 20, 1999, there had been network logins and network operations from a remote computer. Mr. Lucier testified that the firewall log showed that a remote computer with an Internet Protocol (IP) address of 208.155.108.160 had logged onto the TSG network. See Record at 153. Testimony revealed that a computer with the same IP address was found at Mr. **Honhart's** residence. Ultimately TSG had to reinstall its operating systems but only after removing some files from the network server, including a SECEVENT file n3 and the firewall log. Testimony established that a "firewall" is a security system which screens access to a computer network, and the firewall log tracks who logs onto the network and when. See Record at 113-44.

----- Footnotes -----

n2 See infra note 4.

n3 Testimony established that a "SECEVENT" file is a Security Event file that registers activity on the network server. See, inter alia, Record at 130. The user sets the activities logged. See, inter alia, Record at 234-35.

----- End Footnotes-----

Thus, the only evidence of a [**6] cause of any malfunction was the kernel error message seen by Mr. Lucier. The kernel is the core of a computer's operating system. See Record at 166. "[T]he kernel file is... the root of an operating system... [or the] first part [of a machine] from which everything else is built. It's like the frame of your car, and everything else comes after that." See Record at 109 (Scott Lucier's testimony). Testimony established that TSG administrators had access to the kernel file, n4 and a number of these administrators were identified at trial.

----- Footnotes -----

n4 See record at 105-06.

----- End Footnotes-----

Detective James Haughom of the Vienna Police Department testified on behalf of the Commonwealth and his testimony establishing the following:

1. The Defendant accessed the kernel files. See Record at 169.
2. There are a number of processes by which the kernel files may be accessed. See Record at 170.
3. There are reasons to access the kernel files other than to modify them. See Id.

[*159] 4. Haughom could not tell what the defendant did **[**7]** to the kernel files. See Record at 180.

5. Kernel files can be accessed accidentally. See Record at 189.

6. Haughom could not tell the manner in which computer shut down. See Record at 164. n5

----- Footnotes -----

n5 Detective Haughom testified that "if [the network] were shut down remotely that there may be some [repercussions] - it may not have been shut down the way it's supposed to have been shut down and that there could be some repercussions from that... as far as the operating system functioning properly." See Record at 166. This testimony, however, was stricken as speculative.

----- End Footnotes -----

The Commonwealth indicted Mr. **Honhart** under § 18.2-152.4, which provides a long laundry list of illegal and unauthorized activities involving another person's computer. Specifically, by way of its Indictment and Bill of Particulars, the Commonwealth alleged that Mr. **Honhart** used the computer or computer network without authority with the intent to cause the computer to malfunction. See Record at 68-70. It is clear from the evidence presented **[**8]** at trial a reasonable jury could find beyond a reasonable doubt that Mr. **Honhart** was a cause of the computer or computer network shut down on April 20, 1999, at The Signature Group (TSG). The charge in this case, however, is limited to violation of section (A)(2) of the statute, which says, "It shall be unlawful for any person to use a computer or computer network without authority and with the intent to... cause a computer to malfunction regardless of how long the malfunction persists." Va. Code Ann. § 18.2-152.4(A)(2) (emphasis added). In a prosecution under Va. Code Ann. § 18.2-152.4(A)(2) proof of halting a computer alone is insufficient for conviction.

The Commonwealth's burden was to prove that Mr. **Honhart** did more than simply halt another's computer; the evidence had to establish beyond a reasonable doubt that Mr. **Honhart** intended his actions to cause a malfunction of another's machine. In this case, the jury could conclude that the Commonwealth linked Mr. **Honhart's** computer activities to the computer shut down at TSG and that there was an inability of the system to re-boot after the shutdown. However, no direct evidence established that the computer malfunction resulted **[**9]** from the Defendant's or anyone's deliberate act. Further, no direct evidence established that the Defendant intended to cause any malfunction, thus, any evidence of the defendant's intent is circumstantial in nature.

HN2 "The Commonwealth always bears the burden of proving guilt beyond a reasonable doubt. When the Commonwealth relies solely upon [circumstantial] evidence to identify a criminal agent, it bears the burden of **[*160]** excluding every reasonable hypothesis of innocence, that is, those which flow from the evidence itself, and not from the imagination of defendant's counsel." Tyler v. Commonwealth, 254 Va. 162, 487 S.E.2d 221 (1997) (quoting Turner v. Commonwealth, 218 Va. 141, 148, 235 S.E.2d 357 (1977)). The evidence in this case did not exclude the

reasonable hypothesis of innocence that Mr. **Honhart** accidentally adversely effected the kernel. Under controlling authority, the evidence supported a reasonable hypothesis of innocence, therefore the Defendant's Motion to Strike must be granted [and the indictment dismissed].