SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-6044-17

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

JADE STEPHEN EPLIN,
a/k/a JADE S. ELPIN,

Defendant-Appellant.

Submitted September 13, 2021 – Decided October 1, 2021

Before Judges Sumners and Vernoia.

On appeal from the Superior Court of New Jersey, Law Division, Atlantic County, Indictment No. 16-10-2424.

Mark E. Roddy, attorney for appellant.

Cary Shill, Acting Atlantic County Prosecutor, attorney for respondent (John J. Lafferty, IV, Acting Assistant Prosecutor, of counsel and on the brief).

PER CURIAM

Tried by a jury, defendant was convicted of third-degree possession or viewing child pornography, N.J.S.A. 2C:24-4(b)(5)(b)(iii), arising from child pornographic images discovered on his computer when he was a student at Stockton State University. He appeals, arguing:

> POINT I
>
> [DEFENDANT]'S CONVICTION WAS BASED UPON EVIDENCE DERIVED FROM AN ILLEGAL WIRETAP.
>
> POINT II
>
> AN INDIVIDUAL CANNOT CONSENT TO SOMETHING HE DOES NOT KNOW ABOUT.
>
> POINT III
>
> THE TRIAL COURT'S DECISION TO SLAM THE DOOR SHUT ON THE DEFENDANT'S SUPPRESSION HEARING DEPRIVED HIM OF AN OPPORTUNITY TO LITIGATE THE FOURTH AMENDMENT ISSUES IN HIS CASE.
>
> POINT IV
>
> ARTICLE 1, PARAGRAPH 1 OF THE NEW JE[R]SEY CONSTITUTION OF 1947 PROHIBITS A CONVICTION FOR ANY INDIVIDUAL WHO WAS SIMPLY "LOOKING" AT SOMETHING. (Not Raised Below)
>
> POINT V

IT WAS ERROR FOR THE TRIAL COURT NOT TO GRANT THE MOTION FOR JUDGMENT OF ACQUITTAL NOTWITHSTANDING THE JURY VERDICT.

We reject defendant's arguments that his motion to suppress evidence and motion for acquittal should have been granted. We conclude that his acceptance of the University's computer acceptable use standards policy in employing its server to access the internet gave the University the right to monitor his computer and retain the child pornographic images linked to his computer. We further conclude that there was sufficient evidence from those images as well as testimony presented by the State's witnesses for the jury to find defendant guilty of possession or control of child pornography.

We begin by addressing defendant's contention that the child pornographic images linked to his computer through the use of the University's computer server should have been suppressed because the seizure violated his privacy rights under the Fourth Amendment of the U.S. Constitution and Article 1, paragraph 7 of the N.J. Constitution against unreasonable search and seizure of information linked to his computer. He maintains that the University's interception and recording of his internet activity constituted a "wiretap" because his internet activity is a "wire communication" under N.J.S.A. 2A:156A-2(a). He stresses that because the University was operating at the

behest "of the police and the prosecutor's office" without obtaining a "wiretap order," the University's wiretap was illegal. He contends he did not consent to the wiretap of his internet activity because he was unaware the University was monitoring his internet use. He adds that "consent has absolutely no place in a wiretap analysis."

Defendant's contentions erroneously equate the University's conduct with wiretapping. The University's monitoring of defendant's internet activity when he used its computer server was not a wiretap. The motion judge properly applied the University's acceptable use standards policy in finding the University had the right to monitor defendant's internet activity because he consented to the University's access when he employed its server to go onto the internet.

In her oral decision, the motion judge found support in the following pertinent parts of the policy,[1] stating:

> "Authorized use of an access to [U]niversity's computing and communications facilities is intended and permitted solely to support legitimate educational, administrative, and mission-centered institution."

[1] The record before us does not provide a full copy of the University's acceptable use standards policy.

> And this is in bold. "The [U]niversity may regularly review access logs of servers and network devices to ensure appropriate utilization."
>
> Standard (1) of this appropriate use [policy] says as follows: "(1) Forms of expression that are not protected by First Amendment and, therefore, are subject to appropriate restrictions and/or referral to authorities by the [U]niversity include obscene material, child pornography, or other material that violates local, state, or federal statutes."
>
> And I'm reading this directly from the privacy standard. Standard (3) says as follows: "Appropriate use of accessible materials. The [U]niversity reserves the right to inspect the content of electronic files when it has reasonable belief that the content of material would violate university policy, state[,] or federal law. The [U]niversity retains the right to review the content of any files when the content of such files is likely to be material to the alleged violation or in a death, illness, or separation of a user. The contents of the [U]niversity's email and electronic communication systems may be subject to disclosure under subpoena or other written request made pursuant to authorized procedures, including requests made pursuant to the Open Public Records Act."
>
> [Emphasis added.]

The judge further noted that in using the University's server to access the internet, "defendant does not have to agree to the terms in the agreement, simply — [he] had the opportunity . . . to disagree with the terms of the agreement simply by not using the [U]niversity's network."

Defendant does not argue that he accessed the internet from a non-University server. Because he was on notice that the University—to ensure compliance with its internet acceptable use standards policy—had the right to review his internet activity when he used its server, there was no violation of defendant's federal or state constitutional rights. Defendant accordingly had no expectation of privacy given his acceptance of the University's policy. There was no restriction on the University recording and sharing with the State what it obtained when monitoring defendant's internet use.

In sum, the motion judge's factual findings are supported by credible evidence in the record, see State v. Lamb, 218 N.J. 300, 313 (2014) (citing State v. Elders, 192 N.J. 224, 243 (2007)), and we discern no basis to upset the denial of defendant's suppression motion.

We also see no merit to defendant's argument that he was entitled to an evidentiary hearing to determine his motion to suppress, and that we should reverse "[his] conviction and direct the trial court to conduct a full evidentiary hearing on the facts and circumstances surrounding the wiretap." Based on the record provided, defendant never made a request for a hearing. When the judge asked defense counsel to state, "what you're seeking and why you're seeking it," counsel gave a factual synopsis of how the University obtained the child

pornographic images linked to defendant's computer, acknowledging "[t]here's actually not much [facts] in dispute," and why it violated defendant's privacy rights. Because there was no request for a hearing, we review for plain error. State v. Santamaria, 236 N.J. 390, 404 (2019) (citing R. 2:10-2).

Defendant fails to establish that there were material facts in dispute that needed to be resolved in an evidentiary hearing. See State v. Green, 346 N.J. Super. 87, 90-91 (App. Div. 2001) (holding that mere allegation of a warrantless search, coupled with the State's burden to justify it, does not constitute a material dispute of fact requiring an evidentiary hearing). The judge maintained the sole issue in the motion was whether defendant had a privacy expectation from using the University's server. And, as noted above, we agree with her that the University's monitoring of defendant's computer was permissible because he accepted the University's acceptable use standards policy, which allowed it to monitor his activity when he accessed its server to go onto the internet.

Finally, we reject defendant's contention that the trial judge—who did not decide the motion to suppress—erred in not granting the motion for acquittal because "the State's proofs did not rise to the level of proof beyond a reasonable doubt." Specifically, defendant argues the State failed to prove that he possessed or observed the child pornographic images linked to his computer. He also

maintains, for the first time, the Legislature did not criminalize someone for "merely 'looking at something,'" apparently referring to the child pornographic images.

When reviewing a trial judge's denial of a motion of acquittal, we consider whether "based on the entirety of the evidence and after giving the State the benefit of all its favorable testimony and all the favorable inferences drawn from that testimony, a reasonable jury could find guilt beyond a reasonable doubt." State v. Williams, 218 N.J. 576, 594 (2014) (citing State v. Reyes, 50 N.J. 454, 458-59 (1967)). That deferential standard was met here.

In accordance with N.J.S.A. 2C:24-4(b)(5)(b)(iii), "[a] person commits a crime of the third degree if he knowingly possesses, knowingly views, or knowingly has under his control, through any means, including the Internet, less than 1,000 items depicting the sexual exploitation or abuse of a child." Our review of the trial record informs us that the State presented sufficient evidence for the jury to find defendant possessed or had control over child pornographic images in violation of the statute.

Defendant's friend Katherine Cairns testified that while she was in defendant's dormitory room, she declined his offer to see child pornography he had on his computer. Defendant, majoring in computer science, further told

Cairns he had the capability to change his computer's IP address so that when he viewed child pornography, there would be no indication that it was on his computer.

After Cairns reported her conversation with defendant to the University police, Robert Heinrich, the University's Chief Information Officer in charge of the Division of Information Technology Services, was instructed to monitor defendant's internet activity. Heinrich directed Brian Gormley, the University's Associate Director of Network Telecommunications and Network Infrastructure, to monitor defendant's internet activity and network traffic, and to "maintain those logs." Heinrich also testified about the University's acceptable use standards policy.

A three-month investigation ensued, resulting in Gormley finding that defendant encrypted his network traffic, which prevented—except occasionally—Gormley from observing defendant's internet searches and viewings on the University's network. However, Gormley was eventually able to view a large amount of child pornography that was accessed by defendant's computer. He collected the data from the University's network, kept it on a separate server in its original format, and turned it over to the Atlantic County Prosecutor's Office. Gormley could neither confirm that defendant accessed

specific photos after the child pornographic website was accessed nor that defendant accessed any of the thumbnails of pornography depicted on the website.

Through the testimony of Prosecutor's Office Detective Christopher Hallett, the State displayed thirty-five files of individual thumbnails of child pornographic images that Gormley testified were accessed by defendant's computer through the University network. Hallett stated that after defendant's computer and cell phone were seized, an encryption software running on defendant's computer was discovered, which prevented anyone from locating what was on his computer.

Defendant did not testify, nor did he present any witnesses. His arguments that the State's evidence did not prove his guilt beyond a reasonable doubt are unconvincing. Contrary to defendant's contention, his conviction was not based on the State's assertion that he viewed child pornographic images, but as evinced by this use of the University's network, the aforementioned State's evidence clearly showed that he possessed or controlled child pornographic images as prohibited by N.J.S.A. 2C:24-4(b)(5)(b)(iii). The motion for acquittal was properly denied.

Affirmed.