

**NOT FOR PUBLICATION WITHOUT THE APPROVAL
OF THE COMMITTEE ON OPINIONS**

SUPERIOR COURT OF NEW JERSEY
LAW DIVISION—CRIMINAL PART
MERCER COUNTY
INDICTMENT NO. 08-09-0802

STATE OF NEW JERSEY.

Criminal Action

Plaintiff,

v.

DECISION

SERGEANT KENNETH RILEY,

Defendant.

APPROVED FOR PUBLICATION

February 9, 2010

COMMITTEE ON OPINIONS

Decided: October 30, 2009

Doris Galuchie, Deputy First Assistant Prosecutor, for plaintiff (Joseph L. Bocchini, Jr., Mercer County Prosecutor, attorney).

Jeffrey G. Garrigan for defendant (Cammarata, Nulty & Garrigan, L.L.C., attorneys).

OSTRER, J.S.C.

Under New Jersey's computer crime law, a person commits a third degree crime if he knowingly or purposely accesses computerized data without authorization or in excess of authorization. N.J.S.A. 2C:20-25(a). A person also commits a third degree crime if he so accesses data and then knowingly or recklessly discloses it. N.J.S.A. 2C:20-31(a). Defendant's motion to dismiss the indictment requires the court to determine, as a matter of first impression, whether the law covers employees who enjoy password-protected access to computerized information, but who view or use such information in ways or for purposes that their employer prohibits.

The court concludes that the statute does not reach that far. Therefore, the court shall dismiss the indictment, which charges computer crimes based on unauthorized access, as well as official misconduct predicated on the alleged computer crimes. The court has relied on the statute's plain language, legislative history, related case law, persuasive out-of-state authority, and scholarly commentaries. The court's statutory construction also conforms to the rule of lenity, and avoids unconstitutional vagueness.

BACKGROUND

The grand jury returned a six-count indictment against defendant on September 12, 2008. Defendant is charged: in counts one and four with computer criminal activity (third degree); in counts two and five with unlawful access and disclosure of computer data (third degree); and in counts three and six with official misconduct (second degree).

On each of two days, January 6 and 9, 2008, defendant allegedly "purposely or knowingly, and without authorization or in excess of authorization, access[ed] ... data, [a] data base, or computer storage medium" contrary to N.J.S.A. 2C:20-25(a); and he "purposely or knowingly, and without authorization or in excess of authorization, access[ed] ... data, [a] data base, or computer storage medium, and did knowingly or recklessly disclose such data" contrary to N.J.S.A. 2C:20-31(a). In so doing, each time, he committed an act of official misconduct, by accessing the Mobile Vision Recorder ("MVR") data base in excess of his authorization, with the purpose to injure fellow Sergeant Robert Currier. In so doing, he allegedly violated N.J.S.A. 2C:30-2(a), which makes it an offense for a public servant to commit an act relating to his office, with the purpose to injure another (or benefit himself), knowing that such act is unauthorized or he is committing such act in an unauthorized manner.

For the purposes of deciding the motion, the court will accept the facts as alleged by the State. See State v. Morrison, 188 N.J. 2, 12-13 (2006) (on motion to dismiss indictment, court must consider facts in light most favorable to State). According to the State, defendant twice viewed a digitally stored video of a motor vehicle stop conducted by three other police officers in the early morning hours of January 6, 2008. The stop involved a driver suspected of driving under the influence of intoxicating liquors. Participating in the stop were Princeton Borough Police Sergeant Robert Currier, and Patrolmen Garrett Brown and William Perez. Also near the scene was Patrolman Mervyn Arana. Brown and Arana were assigned to defendant's squad at the time, and subject to his general supervision. Brown assisted Currier with the motor vehicle stop. During the stop, Currier allowed the suspect to urinate in nearby bushes.

The video was recorded on a computerized system that automatically downloaded digitally recorded traffic stops to the Borough Police Department's computer system. All sergeants, including defendant, had passwords that enabled them to view any such digital recordings. According to one witness, the only practical way to enter the computer system containing the recordings was to use "an administrative officer's password or a sergeant's password." A sergeant could use his password to access the entire MVR database. Defendant learned of the permitted urination, and believed that Currier had violated law and policy. The grand jury heard testimony that defendant disliked Currier and wished him ill.

The State presented evidence that defendant used his password to view the recording of the traffic stop on January 6, 2008 and January 8, 2008. He also permitted police personnel below sergeant's rank to view the video. And his motivation for doing

so, according to evidence viewed favorably for the State, was not to train officers in his own squad, but to cause injury to Carrier, by subjecting him to embarrassment and discipline. Evidence also was presented that defendant attempted to mislead superiors about when and why he viewed the video of the traffic stop.

The State also presented evidence that defendant violated the department's policy and procedures for the proper use of mobile video and audio equipment ("MVR Policy"). The MVR Policy requires sergeants, as members of supervisory personnel, to review "routine" digital video recordings involving their subordinates for training purposes. This requirement is found in the policy's section on supervisors' responsibilities:

Supervisory personnel shall ensure the following:

-
- b. They review randomly selected "Routine" videotapes and DVR computer file recordings for each subordinate for whom they conduct an evaluation. The review will assist the supervisor in assessing the officer's job performance in this area and will additionally help determine if the MVR equipment is being fully and properly used. Deficiencies shall be addressed/corrected by the supervisor and then reported to the training officer for possible additional training needs. Material that may be appropriate for training may also be identified at this time. Tapes for this purpose should be requested from the Patrol Lieutenant.

[MVR Policy, § III(C)(1)(b)].

The requirement is also found in the policy's section on qualitative review:

Supervisors review

- a. As per this policy and procedure, sergeants shall periodically review "ROUTINE" tapes and DVR computer files, which will provide an excellent foundation for an assessment of an officer's performance regarding certain criteria.

[MVR Policy, § III(F)(2)(a)].

A tape is deemed “Routine” if it is “apparent at the time of retrieval that there . . . is nothing recorded on the tape that is considered evidentiary or worthy of further documentation.” MVR Policy, § III(B)(2)(f)(2)(a).

The policy also authorizes a “Traffic/Support Services Sergeant” to write files to CDs or DVDs. “If evidence or criminal activity is captured on a DVR unit, [an officer shall] notify the Patrol Lieutenant or the Traffic/Support Services Sergeant so they can have the files written to a CD or DVD. The CD or DVD shall then be stored in accordance with the departments [sic] current evidence procedure.” MVR Policy, § III(B)(2)(g)(5). As the State concedes, “the policy clearly entitles the defendant to access the database in order to download the videos of his subordinates to CDs or DVDs.”

As interpreted by grand jury witnesses, the policy’s explicit grants of authority to sergeants were exclusive of any other authority. Thus, the policy only permitted sergeants to view tapes randomly of their subordinate officers for training purposes. They could not view tapes for any other purpose. They could not even view a tape of a subordinate while acting under the command of another sergeant. Also, the policy prohibited a sergeant from accessing a recording of another sergeant’s stop.

The State argues that defendant gained entry to the MVR database, and viewed the recordings of Currier’s stop, for a purpose not permitted by the MVR Policy. Therefore, he accessed data without authorization or in excess of authorization.

DISCUSSION

The standard for dismissing an indictment is well settled. “A trial court . . . should not disturb an indictment if there is some evidence establishing each element of the crime to make out a prima facie case.” State v. Morrison, supra, 188 N.J. at 12. The

evidence presented need not be sufficient to sustain a conviction. State v. N.J. Trade Waste Ass'n, 96 N.J. 8, 27 (1984). However, where the statute is interpreted in such a way that the facts presented to the grand jury simply do not fall within the statute invoked, then the indictment must be dismissed. See, e.g., State v. Morrison, supra, 188 N.J. at 19-20 (after interpreting drug laws to provide that person cannot distribute controlled dangerous substance to person with whom he shares joint possession, Court dismissed distribution counts of indictment because facts indicated that defendant jointly possessed drugs with alleged distributee).

In interpreting the statute, the court will first review its plain language, concluding that it is ambiguous, requiring resort to extrinsic sources. The court will then discuss its interpretation in light of legislative history, related case law, persuasive out-of-state authorities and commentaries, and the need to comply with the rule of lenity and to avoid constitutional infirmity.

1. The Statutory Language is Ambiguous.

The court will first review the language of the statute, and then discuss alternative interpretations, leading to the conclusion that the statute is ambiguous.

Statutory Language. A person is guilty of computer criminal activity, as charged in counts one and four: “if the person purposely or knowingly and without authorization, or in excess of authorization: (a) Accesses any data, data base, computer storage medium [or] . . . computer” N.J.S.A. 2C:20-25(a). It is a third degree crime. N.J.S.A. 2C:20-25(g). Unauthorized access, in turn, is an element of the law prohibiting unlawful access and disclosure of computer data, as charged in counts two and five. That law makes it a third degree crime “if the person purposely or knowingly and without authorization, or in

excess of authorization, accesses any data, data base, computer, [or] computer storage medium ... and knowingly or recklessly discloses or causes to be disclosed any data....”

N.J.S.A. 2C:20-31(a).

As used in both statutes, “access” is defined to include not simply entry into a computer data base, but also acts of communication, storage and retrieval. It means “to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer storage medium, computer system, or computer network.” N.J.S.A. 2C:20-23(a). Access also includes, as just noted, an act that “otherwise make[s] use of” the computer and data. As discussed below, that additional element conceivably can substantially broaden the meaning of access.

“Authorization” is defined to mean “permission, authority or consent” from the person who is empowered to give permission. It means:

[P]ermission, authority or consent given by a person who possesses lawful authority to grant such permission, authority or consent to another person to access, operate, use, obtain, take, copy, alter, damage or destroy a computer, computer network, ... system, ... equipment, ... software, ... program, ... storage medium, or data.

[N.J.S.A. 2C:20-23(q)].

“In excess of authorization” is not separately defined.¹

¹ It is a defense to a charge of acting without or in excess of authorization, if a reasonable person would have believed he was authorized. “An actor has authorization if a reasonable person would believe that the act was authorized.” N.J.S.A. 2C:20-23(q). The statute does not label this an affirmative defense. So, the State must prove that a reasonable person would not believe he was authorized. See N.J.S.A. 2C:1-13(c).

With respect to mens rea, the Legislature expressly requires proof that the defendant purposely or knowingly gained access to one of the identified computer-related objects. Less clear is whether the defendant must have a particular state of mind regarding the lack of authorization. Arguably, based on general principles of liability, the State must prove that the defendant himself at least knew that he lacked authorization or exceeded authorization. See N.J.S.A. 2C:2-2(c)(3) (“A statute defining a crime, unless

Statutory Interpretation. It is uncertain what it means, first, to access computerized data, and second, what it means to do so “without authorization” or “in excess of authorization.” It is also unclear whether unauthorized access may be proved solely with evidence that a defendant, who is an employee or other “insider” with current password-access, knowingly violated internal guidelines regarding use of computer-based information. (By “unauthorized,” this court refers to actions without authorization or in excess of authorization.)

A hypothetical can demonstrate the uncertainty. One can posit a member of the information technology (I.T.) department of a business who possesses all the employees’ passwords in order to maintain the business’s computer system, but internal policy directs him not to read employees’ documents. In one sense, the I.T. professional is authorized to access every employee’s files. If a worker asks the I.T. professional to help retrieve a sensitive trade-secret-related document that the worker accidentally deleted, the I.T. professional can do so, using the passwords already provided to him. In another sense, if the I.T. professional reads the worker’s document, he may be acting in excess of his authorization. Reference to the plain language of the statute does not clearly indicate which reading is correct.

On one hand, the definitions of “authorization” and “access” can be read broadly to expand the statute’s reach. First, “authorization” can be read to refer not simply to a

clearly indicating a legislative intent to impose strict liability, should be construed as defining a crime with the culpability defined in paragraph b(2) [knowingly].”).

On the other hand, the Legislature has expressly required the State to prove that a reasonable person – as distinct from the defendant – would not believe he was authorized to access the computer-based object. N.J.S.A. 2C:20-23(q). In so doing, perhaps the Legislature intended to impose an objective standard. In other words, regardless of the defendant’s subjective knowledge about the existence of, or scope of authorization, if a reasonable person would know that he lacked authorization or exceeded authorization, then that element of the crime would be satisfied.

password or other code-related powers to enter or utilize a computer, but also to include permission to use information once entry is achieved. “Authorization” is defined to include “permission, authority or consent . . . to access, operate, use, obtain, take, copy, alter, damage or destroy . . . data.” N.J.S.A. 2C:20-23(q). Arguably, although “in excess of authorization” is not specifically defined, it covers someone who accesses a computer with authorization, but then uses data so accessed without authorization. Moreover, the “otherwise make use of” clause in the definition of “access” in the New Jersey law may be broadly construed to cover not simply entry into a database or computer system, but the use of it once entry is achieved.

On the other hand, section 25(a) may – and this court ultimately concludes, should -- be read more narrowly. One may construe “authorization” to refer only to a password, or other code-based restrictions to utilizing a computer. Thus, the I.T. worker posited above did not access the document without, or in excess of authorization. The worker had the password. Thus, he had the “permission, authority or consent” to enter the employee’s document files. While the “authorization” definition refers to permission not only to “access” but also to “operate, use, obtain, take, copy, alter, damage or destroy,” N.J.S.A. 2C:20-23(q), the only kind of unauthorized action that is criminal under N.J.S.A. 2C:20-25(a) is unauthorized “access.” Therefore, according to this narrow reading, the reference to “operate, use, obtain, take, copy, alter, damage or destroy” is not relevant to analysis of Section 25(a).² Also, the worker had authority to

² By contrast, reference to “use, obtain, take, copy, alter” may be relevant to analysis of Section 25(e), which makes it unlawful if a person, “purposely or knowingly and without authorization, or in excess of authorization . . . [o]btains, takes, copies or uses any data, data base, computer program, computer software, personal identifying information, or other information stored in a computer, computer network, computer system, computer equipment or computer storage medium.”

“communicate with” or “retrieve data from” the computer system, to borrow language from the “access” definition. N.J.S.A. 2C:20-23(a).

The worker even arguably had authority to “make use” of the document if “make use” is narrowly construed to encompass actions like retrieving or restoring documents, but not broadly construed to encompass reading them. According to this interpretation, language in the definition of “access” that includes “otherwise make use of” would be read narrowly, to refer to activities similar to those mentioned immediately before – such as computer instructions, communications with computers, data storage and retrieval – in other words, actions closely related to the computer itself. See Gallenthin Realty Dev., Inc. v. Borough of Paulsboro, 191 N.J. 344, 367 (2007) (“Under that canon of statutory interpretation, ‘where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words.’”) (quoting 2A Norman J. Singer, Sutherland Statutory Construction § 47:17 (6th ed. 2000)). Reading a document once retrieved therefore would fall outside the scope of the definition of “access,” and also would fall outside the scope of section 25(a), which criminalizes “access” that is unauthorized.³

Federal law defines the term, “exceeds authorized access,” to mean “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.” 18 U.S.C. § 1030(e)(6).

³ The court notes that N.J.S.A. 2C:20-25(e), quoted in note 1, supra, which is not charged in the indictment, more clearly addresses misuse of computer data. Without using the term “access,” the provision criminalizes unauthorized obtaining, taking, copying or use of various forms of computer-related objects. However, the bounds of that provision are also questionable. If “authorization” is read broadly to go beyond password or code-related permission, to include any kind of permission, then it arguably would be a third degree crime to borrow a person’s Blackberry without permission to send an email. Likewise, it would be a third degree crime for a public library visitor to exceed the library’s two-hour time limit, and obtain unauthorized use of publicly available internet computers.

That also is not unambiguous, as one may ponder what it means to be “not entitled to obtain or alter” data. Arguably, one is entitled if he has a password or code-based right to obtain or alter the data. See Katherine Mesenbring Field, Note: Agency, Code, or Contract: Determining Employees’ Authorization Under the Computer Fraud and Abuse Act, 107 Mich.L.Rev. 819, 834 (2009) (hereinafter “Determining Employees’ Authorization”) (arguing that the definition of “exceeding authorized access” “merely shifts the focus to insider’s entitlement to information or data and fails to explain whether such entitlement is determined by code-based limits to one’s ability to access or by employer-defined limits”).

Significantly, New Jersey did not adopt the federal definition. In N.J.S.A. 2C:20-25(a), “in excess of authorization” simply modifies “access.” Thus, according to a narrow reading, the statute does not cover “use” in excess of authorization. Rather, it covers a situation where someone has password or code-based permission to enter certain databases but not others, but hacks his way into a second level within the computer data base. If the Legislature wanted to cover persons who acted in excess of authorization to use data, as opposed in excess of authorization to access data, it could have said so.

A narrow reading of N.J.S.A. 2C:20-25(a) also may be compelled when the statute is compared to N.J.S.A. 2C:20-31(a), entitled “Wrongful access, disclosure of information.” Counts two and five charge that defendant violated section 31(a). However, if unauthorized access may be proved by an employee simply using, contrary to policy or contract, information that he obtained with current passwords or code-related rights, then section 31(a) is surplusage. See In re Commitment of J.M.B., 197 N.J. 563, 573, cert. denied, ___ U.S. ___, 130 S.Ct. 509, 175 L. Ed.2d 361 (2009) (“Interpretations

that render the Legislature’s words mere surplusage are disfavored.”). Section 31(a) requires proof of two elements: first, that the person “purposely or knowingly, and without authorization, or in excess of authorization, accesses any data, data base, computer....”, and second, that the person “knowingly or recklessly discloses or causes to be disclosed any data, data base, computer software, computer programs or personal identifying information.” The first element is the same as a violation of section 25(a). If section 25(a) is so broadly read that it covers an employee who “otherwise makes use” of data without contractual permission, then the second element of section 31(a) would require no additional proof, as disclosure would be encompassed within the meaning of “otherwise makes use.” Since this court must presume that the second element in section 31(a) was intended to add something substantive, the expansive reading of 25(a) is therefore disfavored.⁴

In sum, the statute’s plain language can be read two ways. This ambiguity justifies resort to legislative history and other extrinsic sources. Twp. of Pennsauken v. Schad, 160 N.J. 156, 170 (1999) (court may consider “statute's purpose, legislative history, and statutory context” to construe ambiguous statute).

2. Legislative History.

The Legislature’s intent can be viewed both specifically – by referring to explicit expressions of intended meaning or purpose – and generally – by considering the evils that the Legislature apparently intended to address. The court will consider these in turn.

⁴ Another “access-plus” crime is found in N.J.S.A. 2C:20-25(f), which makes it a crime for a person, without or in excess of authorization, to access and then recklessly alter, damage or destroy computer data and other specified computer-related objects. The statute perplexingly defines this as a fourth degree crime if the value of damage is \$5,000 or less, although this section includes all the elements of the third degree crime in section 25(a), plus additional elements. N.J.S.A. 2C:20-25(g).

But first, the court must review the history of section 25(a), which criminalizes access to data without or in excess of authorization.

Specific Legislative History. In 2003, the Legislature significantly amended the computer crime law that was first enacted in 1984. L. 2003, c. 39, amending L. 1984, c. 184. Its expressed general purpose was to incorporate recent technological changes; thus, for example, reference to the internet was included in the definition of “computer network” found in N.J.S.A. 2C:20-23(d). L. 2003, c. 39, § 1. “This bill would update the State law with regard to computer crime to reflect various technological changes, including the development of the Internet, that have occurred since enactment of the computer crime law in 1984” Sponsor’s Statement to S.1355 (March 25, 2002).

However, the 2003 amendments did more than just update technology. In the 2003 law, the Legislature made it a crime simply to access data without or in excess of authorization. L. 2003, c. 39, § 3, (codified at N.J.S.A. 2C:20-25(a)). Previously, access alone was an offense if the access was to a “computer system.” A person was guilty of a crime of the third degree “if he purposely and without authorization accesses, alters, damages or destroys a computer system or any of its parts, where the accessing and altering cannot be assessed a monetary value or loss.” L. 1984, c. 184, § 9 (emphasis added), (previously codified at N.J.S.A. 2C:20-30), repealed by, L. 2003, c. 39, § 9. Simple access, without alteration, damage, or destruction, and without a monetary loss, was a disorderly persons offense. L. 1984, c. 184, § 11, (previously codified at N.J.S.A. 2C:20-32), repealed by, L. 2003, c. 39, § 9.

In other words, Section 9 of the 1984 Act applied when simple access caused a monetary loss, albeit not measurable, and section 11 applied when simple access caused

no monetary loss at all. State v. Gaikwad, 349 N.J. Super. 62, 78-79 (App. Div. 2002). Under the 2003 amendments, simple access pertains not only to “computer systems” but also to any “data, data base, computer storage medium, computer program, computer software, computer equipment, computer . . . or computer network.” N.J.S.A. 2C:20-25(a). And, simple access is now a third degree crime regardless of whether there is monetary loss. N.J.S.A. 2C:20-25(g). The 1984 definition of “access” was unchanged in the 2003 law, except for the addition of “computer storage medium” as one of the objects of access. L. 2003, c. 39, § 1, (codified at N.J.S.A. 2C:20-23(a)).

The 2003 amendments also introduced the concept of acting “in excess of authorization” in section 25. L. 2003, c. 39, § 3. However, as noted above, the Legislature did not define “in excess of authorization.” But, for the first time, it defined “authorization” – a term found in the law since 1984, but hitherto undefined. The Senate Judiciary Committee addressed this change: “The committee amendments add a definition of ‘authorization’ to be consistent with federal law and clarify that authorized access in the ordinary course of business is not intended to be reached by the criminal provisions of the bill.” Senate Judiciary Committee Statement to S.1355 (June 13, 2002).

The just-quoted statement of intent is both illuminating and perplexing. It is illuminating because the Committee expressed the intent not to reach access authorized in the ordinary course of business. That arguably reflected an intention not to criminalize the very kind of behavior involved in this case – workplace access enabled by a password, but allegedly used in a way prohibited by internal workplace policies. A U.S. House of Representatives Committee expressed a similar concern about the 1984 version of the federal law. The Committee “did not want to extend the 1984 Act ‘to any type or

form of computer access that is for a legitimate business purpose. Thus, any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected.’” Determining Employees’ Authorization, *supra*, 107 Mich.L.Rev. at 831 (quoting H.R. Rep. No. 98-894, at 21, reprinted in 1984 U.S.C.C.A.N. at 3707).

However, as the Note-writer observes, the meaning of “legitimate purposes” was unclear. Ibid.

On the other hand, the New Jersey Committee’s statement is perplexing because, notwithstanding the expressed intention to include a definition of “authorization” to be consistent with federal law, there is no definition of authorization in the federal statute. Compare 18 U.S.C. § 1030(e) (defining terms). See also Determining Employees’ Authorization, *supra*, 107 Mich.L.Rev. at 838 (“The legislative history of the CFAA clearly establishes that Congress never defined many difficult and confusing, yet key, terms in the CFAA, such as ‘access,’ ‘use,’ and ‘without authorization,’ even in light of repeated pleas for clear definitions.”). Rather, the federal statute only defines “exceeds authorized access.” 18 U.S.C. § 1030(e)(6).

Moreover, the expressed intent to align state law with federal law is perplexing because federal case law reflected inconsistent approaches. See O. Kerr, Cybercrime’s Scope: Interpreting ‘Access’ and ‘Authorization’ in Computer Misuse Statutes, 78 N.Y.U.L. Rev. 1596, 1597 (2003) (hereinafter “Interpreting ‘Access’ and ‘Authorization’”) (“What does it mean to ‘access’ a computer? Under what circumstances does access become ‘unauthorized?’ The few courts that have reached these questions have offered inconsistent interpretations.”). Thus, it is unclear which federal approach that the New Jersey Senate Judiciary Committee found persuasive.

Nonetheless, on balance, given the Committee’s expressed intent not to reach access in the ordinary course of business, the specific legislative history appears to favor narrowly reading “unauthorized access.” In other words, the Legislature apparently did not intend to criminalize the actions of an insider, who enjoys password or code-based access to information, but uses it in a way that violates internal policies.

General Legislative History. The court also finds support for its narrow reading of the law in the general legislative history of computer crime statutes. This court has found no clear evidence that our Legislature intended to address a perceived public policy problem presented by employees who enjoy password-based access to their workplace computer systems, but violate internal workplace computer policies, at least absent some additional harm, such as fraud, theft of trade secrets or other proprietary information, or malicious destruction of data or computer systems.

As Kerr argues, the federal and state computer crime laws were first enacted in the late 1970s to address “perceived failures of preexisting laws to respond to computer misuse.” *Id.* at 1602. He distinguishes between two kinds of “computer crimes:” (1) traditional crimes, such as theft, pornography trafficking, committed using computers, and (2) the crime of computer misuse. The latter necessitated the new laws. “We can define computer misuse as conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks. Common examples include computer hacking, distribution of computer worms and viruses, and denial-of-service attacks.” *Id.* at 1603-04. See also *Determining Employees’ Authorization*, supra, 107 *Mich.L.Rev.* at 835-36, 839 n.123 (describing

Congressional concerns over the years with hackers, pirate bulletin boards, stolen passwords, worms and viruses, and terrorists).

The shortcomings of existing theft and trespass laws to reach this latter form of computer misuse led to the enactment of computer crime legislation. “The uncomfortable fit between computer misuse and traditional property crimes triggered a great deal of commentary in the late 1970s and early 1980s about the need for computer crime legislation.” Interpreting ‘Access’ and ‘Authorization’, *supra*, 78 N.Y.U.L. Rev. at 1613. Kerr notes that the federal law and every state law “share the common trigger of ‘access without authorization’ or ‘unauthorized access’ to computers.” Id. at 1615. In most jurisdictions, unlike in New Jersey, unauthorized access is not itself a crime, but is an essential element of other offenses. Ibid.

Kerr argues that the general legislative intent was to model the computer crime law to trespass and burglary laws. “It is impossible to . . . know what . . . [legislators] had in mind when they enacted unauthorized access computer crime statutes. Still, the available evidence suggests that legislators mostly saw such statutes as doing for computers what trespass and burglary laws did for real property.” Id. at 1617.

Concededly, Congress at some point recognized that the law should reach the actions of malicious insiders. However, it failed to clarify who it covered and for what.

Determining Employees’ Authorization, *supra*, 107 Mich.L.Rev. at 840 (“Congressional ambiguity and even confusion about insider authorization in the CFAA also suggests a congressional determination to leave the authorization question to courts.”).

In sum, the general legislative history supports a narrow reading of section 25(a). The court should tailor its interpretation to the statute’s overarching purpose. Couri v.

Gardner, 173 N.J. 328, 339 (2002). There is no evidence that the New Jersey Legislature had targeted the violation of internal workplace computer policies by persons with current password-based or code-based rights to those workplace computers, at least absent some additional specified harms.

3. The Court's Interpretation Is Consistent with Relevant New Jersey Case Law.

In this court's view, unauthorized access under sections 25(a) and 31(a) does not encompass entry into a computer database by an insider with a current password. This interpretation is consistent with relevant case law interpreting comparable language under the wiretap statute, and is not inconsistent with a case applying the 1984 version of New Jersey's computer crime law.

In White v. White, 344 N.J. Super. 211 (Ch. Div. 2001), the court narrowly construed the New Jersey Wiretap Act, N.J.S.A. 2A:156A-27(a), which, like the computer crime law, prohibited access without authorization. The wiretap law states:

A person is guilty of a crime of the fourth degree if he (1) knowingly accesses without authorization a facility through which an electronic communication service is provided or exceeds an authorization to access that facility, and (2) thereby obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage.

[N.J.S.A. 2A:156A-27(a)].

In White, a wife had retrieved her husband's stored e-mails to a girlfriend from the family computer. The court held that the wife's access was not unauthorized because she did not use her husband's password or code without permission.⁵ In other words, unauthorized access meant access by use of another's password or code-based right of entry.

⁵ The court also held that e-mails stored on a family computer's hard drive were not "communication[s] . . . in electronic storage." White v. White, *supra*, 344 N.J. Super. at 220.

It has been held that “without authorization” means using a computer from which one has been prohibited, or using another’s password or code without permission. Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817 (E.D. Mich. 2000). Although she did not often use the family computer, defendant had authority to do so. Additionally, defendant did not use plaintiff’s password or code without authorization. Rather, she accessed the information in question by roaming in and out of different directories on the hard drive. As stated in Sherman, where a party “consents to another’s access to its computer network, it cannot claim that such access was unauthorized.” Id. at 821.

[White v. White, *supra*, 344 N.J. Super. at 221].

The same reasoning should apply when interpreting the prohibition against unauthorized access in the computer crime law. Although not expressly addressed by the court, presumably there was an implicit agreement between the spouses that they would not read each other’s personal mail. Ms. White violated that implicit agreement, but did not evade a password-based barrier. Concededly, unlike the computer crime law, the wiretap statute does not contain an explicit definition of “authorization.” Nonetheless, this court finds the reasoning in White persuasive.

This court’s interpretation of access “without, or in excess of authorization,” is consistent with the only reported decision under the New Jersey computer crime law, which involved a conviction for, among other things, unauthorized access where the defendant impersonated authorized users, and utilized a revoked user name and password to infiltrate the computer systems of his former employer. State v. Gaikwad, *supra*, 349 N.J. Super. at 72-73. Although the Gaikwad court did not address the issue presented in this case – whether the statute reaches an insider who has current password or code-based permission to enter a current employer’s computer system – the decision highlights the

kind of “hacker” case for which, as discussed above, computer misuse statutes across the country were generally designed to address.⁶

4. A Narrow Reading of the Statute Is Compelled by the Rule of Lenity, and the Void for Vagueness Doctrine.

This court’s narrow construction of sections 25(a) and 31(a) conforms to the doctrine of lenity – the rule that remaining ambiguity in criminal laws must be resolved in defendant’s favor -- and avoids constitutional infirmity based on the void-for-vagueness doctrine. Persons must receive fair warning that certain behavior is criminal. “Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed.” McBoyle v. United States, 283 U.S. 25, 27, 51 S. Ct. 340, 341, 75 L. Ed. 816, 818 (1931) (Holmes, J.).

Fair warning is furthered by the void-for-vagueness doctrine and the doctrine of lenity. United States v. Lanier, 520 U.S. 259, 266, 117 S. Ct. 1219, 1225, 137 L. Ed.2d 432, 442-43 (1997) (stating that fair warning requirement is manifest in the vagueness doctrine, the rule of lenity, and the rule that a court may not add a gloss to an unclear statute that was not apparent from the face of the statute or prior judicial decision). See also State v. Gelman, 195 N.J. 475, 482 (2008) (stating that doctrine of lenity is based on principle that a person is entitled to fair warning of a criminal law’s reach).

⁶ In Gaikwad, the defendant was a former AT&T contract employee who was then working for a competitor. He entered his former employer’s computer system using a password and user name that was “locked out” after AT&T terminated him. Defendant alleged that his former AT&T supervisor had permitted him to enter the AT&T computer system, even after he left AT&T. The jury found defendant guilty of unauthorized access pursuant to now-repealed L. 1984, c. 184, § 9, then found at N.J.S.A. 2C:20-30. The appellate court found that the evidence amply supported the jury’s verdict, based on the defendant’s “attempts to access systems within the AT&T system to which he did not have access even when he was an employee,” his “access of the individual electronic mail of co-workers with whom he had never worked,” and his entry into the AT&T computer system through unusual routes. Id. at 84.

As discussed above, the New Jersey statute on computer access without or in excess of authorization is ambiguous. Neither the statute's plain language, nor its legislative history, clearly compels a broad reading of the statute that supports the State's indictment. Under such circumstances, this court must construe the statute strictly, against the State and in favor of defendant. Ibid.; State v. Reiner, 180 N.J. 307, 318 (2004). A strict construction, favoring defendant, would limit the concepts of "without authorization," and "in excess of authorization," by construing "authorization" to refer to password or code-based rights.

A broader construction would likely run afoul of the vagueness doctrine as well. Indeed, defendant urges this court to find the statute unconstitutional on vagueness grounds. The vagueness doctrine does not address the uncertainty that may arise in determining whether a particular defendant did or did not violate his internal computer use policies that form the basis of the unauthorized access charge. That is a fact issue for a jury. The vagueness issue pertains to whether the statute reaches violations of such policies in the first place, and if so, which ones. However, this court's interpretation of the statute avoids any such constitutional infirmity. See, e.g., State v. Fortin, 198 N.J. 619, 631 (2009) (stating that court "should interpret . . . statute in a manner that would avoid constitutional infirmities, if [it] . . . fairly can do so").

The vagueness doctrine is compelled by notions of due process. State v. Cameron, 100 N.J. 586, 591 (1985); State v. Lashinsky, 81 N.J. 1, 17 (1979). This court does not view the prohibition against unauthorized computer access to be impermissibly vague in all cases, such that it is susceptible to a facial challenge. See State v. Cameron, supra, 100 N.J. at 593 (describing concept of facial invalidity). However, if extended

beyond cases where persons exceed, evade or foil password or code-based rights, the law “does not with sufficient clarity prohibit the conduct against which it sought to be enforced.” Ibid. To paraphrase State v. Lashinsky, supra, 81 N.J. at 18, a person of common intelligence, would not be reasonably apprised that it is a serious crime to violate internal workplace policies on using computers to which the employee has password or code-based rights.

In considering the void-for-vagueness challenge, the extent of the court’s scrutiny and the statutory clarity required “will depend on the purpose of the statute, the context in which the law is challenged, the conduct that is subject to its strictures, the nature of the punishment that is authorized, and, finally, the potential impact of the statute upon activities and interests that are constitutionally protected.” State v. Cameron, supra, 100 N.J. at 594. Applying those standards, the statute would be vague if applied to persons like defendant. There is no evidence that the general purpose of the statute was to address mere workplace violations of internal policies, absent additional harms, such as fraud, trade secret theft, or damage to the computers. That factor favors a narrow construction of the statute.

Also, defendant challenges a law that was substantially revised in 2003. No New Jersey court in a published decision has interpreted or applied the law to the kind of conduct with which defendant is charged: violation of internal computer policies by an employee with current password access. The unprecedented nature of the prosecution also supports a vagueness challenge based on the absence of fair warning.

As noted above, Cameron, supra, 100 N.J. at 594, also requires the reviewing court to consider the nature of the punishment. See also State v. Afanador, 134 N.J. 162,

170 (1993) (severe sentence warrants closer scrutiny in vagueness challenge). Someone might well anticipate some civil consequences for violating internal workplace computer use policies. However, it is unlikely that one would anticipate third degree sanctions, or worse, a mandatory five-year prison sentence if the violation occurs in the exercise of a public servant's duties, and the criminal computer access forms the basis of an official misconduct charge. That severe punishment supports a narrow construction of the law.

The State's prosecution depends on reading the computer crime act to criminalize what amounts to breach of employment contracts, or even less formal employment policies, governing use of workplace computers by insiders or employees already granted some level of access to them. In effect, according to the State, the criminal law has incorporated by reference those often unclear and informal workplace policies. Actual notice to employees, let alone their explicit acceptance, is often non-existent.

This court's decision to reject so broad a reading of the statute finds support in the appellate court's decision in State v. Lisa, 391 N.J. Super. 556, 579-80 (App. Div. 2007), aff'd, 194 N.J. 409 (2008). In that case, the court dismissed a manslaughter indictment, holding that the criminal law's incorporation, in N.J.S.A. 2C:2-1(b)(2), of principles on duty to act, derived from civil common law, did not provide sufficient notice to satisfy due process. Likewise, incorporating duties to act derived from workplace computer policies would deny a defendant fair warning.

Lastly, the vagueness doctrine assures not only fair warning or notice, but also guards against arbitrary or unpredictable law enforcement. "[T]he Court has more recently noted that the more important aspect of the vagueness doctrine is not actual notice, but the other principle element of the doctrine – the requirement that a legislature

establish minimal guidelines to govern law enforcement.” State v. Reevey, 213 N.J. Super. 37, 44 (App. Div. 1986) (citations and internal quotations omitted). See State v. Golin, 363 N.J. Super. 474, 482-84 (App. Div. 2003) (declaring unconstitutionally vague penal ordinance because it was subject to arbitrary or discriminatory enforcement); Betancourt v. Town of W. New York, 338 N.J. Super. 415, 423-24 (App. Div. 2001) (finding curfew ordinance unconstitutionally vague because it granted police unduly broad discretion).

A key fact affecting the risk of arbitrary enforcement is the prevalence of potential or arguable violations. In State v. Golin, supra, 363 N.J. Super. at 478, the defendant was charged with maintaining a public nuisance because branches of her trees were hanging over and allegedly obstructing a sidewalk in suburban East Windsor. Defendant alleged that tree branches obstructed sidewalks throughout the township. Ibid. The court held that the general ordinance barring a public nuisance did not adequately warn residents that the placement of their trees could prompt sanctions. As a result, the residents were vulnerable to arbitrary or discriminatory enforcement. Id. at 484-85.

In considering the potential for arbitrary enforcement of the computer crime law, this court recognizes the ubiquity of computers today in the workplace, in schools, public institutions, and in government, and the prevalence of agreements and policies governing such use. Many of these impose unrealistic rules honored in the breach. It takes no imagination to conjure up a multitude of trivial and not so trivial violations that take place every day in the workplace. Workers use workplace computers for personal use in violation of requirements that they use their computers for business only. Workers violate policies prohibiting access to social networking sites. Reportedly, fifty-four

percent of companies ban workers from accessing social networking sites like Twitter, MySpace and Facebook, yet seventy-seven percent of workers with a Facebook account use it during work hours. S. Gaudin, Study: 54% of companies ban Facebook, Twitter at work, Computerworld (Oct. 6, 2009), available at [http://www.computerworld.com/s/article/9139020./Study 54 of companies ban Facebook Twitter at work](http://www.computerworld.com/s/article/9139020./Study_54_of_companies_ban_Facebook_Twitter_at_work).

Other violations of internal policies are conceivable. Library users may abuse a policy on public internet computers by staying online too long, or visiting prohibited sites. An employee might share company data with co-workers or family members who are not supposed to see the data (but who do not further disclose it). Concededly, defendant is charged with actions that one might view as more serious. The police department's policies regarding use of MVRs were designed in part to maintain the integrity of evidence. However, there was no allegation that the evidence in this case was damaged or impaired in any way, or that defendant Riley compromised the State's ability to prosecute the driver in Sergeant Currier's motor vehicle stop.

In sum, assuming that a broad range of the population violates internal workplace computer use policies at one point or another, then deeming such violations a crime would empower the State, unguided by firm definitional standards, to choose to prosecute whomever it wishes from that broad cross-section of the population. The vagueness doctrine is designed to prevent that. In short, the criminal law should not be some pliable material that the State may bend and mold at will to fit an unwarned defendant. To avoid a vagueness challenge, the court has narrowly construed the statute as set forth above.

5. Persuasive Authority from Other Jurisdictions and Commentators.

This court's conclusion finds support in scholarly commentaries and persuasive authority from other jurisdictions. According to surveys of federal and state cases construing federal and state computer crime laws, the courts have pursued several distinct approaches to determining whether an insider's or employee's access is unauthorized or exceeds authorization. One school of thought refers to agency principles and scope of employment. If an employee's use of data exceeds the scope of his agency, then the law applies. See Interpreting 'Access' and 'Authorization', *supra*, 78 N.Y.U.L. Rev. at 1633-1637 (discussing cases); Determining Employees' Authorization, *supra*, 107 Mich.L.Rev. at 823-25 (same). See, e.g., Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121 (W.D. Wash. 2000) (adopting agency approach). Other courts ground their decision about whether access is unauthorized by looking to contracts governing use – including employment contracts and contracts with internet service providers. Interpreting 'Access' and 'Authorization', *supra*, 78 N.Y.U.L. Rev. at 1637-40 (discussing cases); Determining Employees' Authorization, *supra*, 107 Mich.L.Rev. at 827-29 (same). Kerr also identifies another school of thought, based on notions of “intended function,” in other words, access was unauthorized if the person used a function in an unintended way to access a computer. Interpreting 'Access' and 'Authorization', *supra*, 78 N.Y.U.L. Rev. at 1629-32.

Lastly, some courts limit the notion of unauthorized access to instances where the person uses a stolen password, or bypasses the password or other code-based barrier to access. Determining Employees' Authorization, *supra*, 107 Mich.L.Rev. at 825-27 (discussing cases). Kerr persuasively argues that a code-based definition of unauthorized

access is most desirable. Interpreting ‘Access’ and ‘Authorization’, supra, 78 N.Y.U.L. Rev. at 1648-60. He notes that many cases that broadly construe the concept of unauthorized access involve civil claims under the CFAA, where courts may be more willing to read a statute expansively. Id. at 1641-42. Therefore, those precedents may be less persuasive in analyzing a criminal law. See State v. Afanador, supra, 134 N.J. at 170 (“[C]ourts give criminal laws sharper scrutiny and more exacting and critical assessment under the vagueness doctrine than they give to civil enactments.”).

This court finds persuasive those decisions that adhere to the narrow interpretation of the federal prohibition of access without or exceeding authorization. See U.S. Bioservices Corp. v. Lugo, 595 F. Supp.2d 1189, 1192-94 (D. Kan. 2009) (after extensively reviewing competing interpretations in case law, court finds that CFAA does not reach employees who, while still employed by plaintiffs, utilized permitted access to obtain confidential information that they then disclosed to competitor); Black & Decker (US), Inc. v. Smith, 568 F. Supp.2d 929, 933-36 (W.D. Tenn. 2008) (after comprehensive review of case, court concludes that statute does not reach misuse of information to which defendant had access); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966, 967 (D. Ariz. 2008) (stating that “the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information,” the court construes “exceeding authorized access” to refer to an insider who has access to some information, but not other information); Diamond Power Int’l v. Davidson, 540 F. Supp.2d 1322, 1343 (N.D. Ga. 2007) (“[A] violation does not depend upon the defendant’s unauthorized use of information, but rather upon the defendant’s unauthorized use of access.”); Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Matsuda, 390 F. Supp.2d 479, 498 (D. Md. 2005) (although defendant “breached the

Registration Agreement by using the information obtained for purposes contrary to the policies established . . . it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization. . . .”).

State authority also supports this court’s narrow construction of unauthorized access. See Gallagher v. State, 618 So. 2d 757, 758 (Fla. Ct. App. 1993) (Glickstein, J., dissenting) (arguing that Florida law, which criminalized computer access without authorization, should not reach non-uniformed police employee, who “had authority to access the . . . NCIC/FCIC system,” when she used the system, in violation of policy, to check if her boyfriend had a criminal record, stating, “[t]he legislature prohibited ‘access,’ not ‘use’”); Briggs v. State, 704 A. 2d 904, 905 (Md. Ct. App. 1998) (reversing conviction for access of computer “without authorization,” where employee was “entitled to use an employer’s computer system in connection with employment duties, but who exceed[ed] the scope of that authorization”); State v. Washington, 710 N.E. 2d 307, 316-17 (Ohio Ct. App. 1998) (albeit in dictum, Court expressed concerns about prosecution of persons for violating employer’s scope of consent to use computer, such as writing personal letter on workplace computer, stating that “the statute may lack sufficient standards to prevent arbitrary and selective enforcement of the statute.”); State v. Olson, 735 P. 2d 1362, 1365-66 (Wash. Ct. App. 1987) (finding that police officer’s print-out of female student photos from University of Washington Police Department computer constituted violation of internal policy on use of data, not unauthorized access).

The court in Olson ordered the dismissal of the charges, notwithstanding that the Washington statute’s definition of “access,” like New Jersey’s, includes the “otherwise make use of” language. The court analogized to trespass laws. “The general trespass

statutes criminalize the entering and remaining upon premises when not licensed, invited, or privileged to enter or remain. By analogy, the computer trespass statute criminalizes the entry into the computer base, not the use of the information obtained.” Id. at 1364.⁷

In sum, although there is a split among other jurisdictions, there is ample precedent in federal and state courts for adopting the narrow construction of “without or in excess of authorization” found in the New Jersey law.

6. In View of the Court’s Statutory Interpretation, The Indictment Must Be Dismissed.

Given this court’s conclusion that the New Jersey computer crime law does not reach defendant’s actions, even after viewing the facts most favorably to the State, counts one, two, four and five shall be dismissed.⁸

⁷ Concededly, neither the Florida, Maryland, nor Washington statutes included the concept of “in excess of authorization” that was added to New Jersey law in 2003.

⁸ For publication, the court has omitted its discussion of the motion to dismiss the official misconduct counts of the indictment.