The Cherokee Supreme Court

Eastern Band of Cherokee Indians
Qualla Boundary, Cherokee, North Carolina

EASTERN BAND OF CHEROKEE INDIANS, APPELLEE,	)	
Vs.	)	FILE NO. 21-CSC-03
BENJAMIN CODY LONG, APPELLANT.	)	

Attorney General Michael W. McConnell, Tribal Prosecutor Cody White, and Associate Counsel Christian N. Siewers, Jr., for the Eastern Band of Cherokee Indians.

Devereux & Banzhoff, PLLC, by Andrew B. Banzhoff, for Defendant-Appellant.

Per Curiam.

Defendant appeals his jury conviction for misuse of Tribal property for accessing network resources belonging to the Eastern Band of Cherokee Indians after being relieved of his duties and put on paid administrative leave from his position as the lead systems administrator for the Tribe's Office of Information and Technology. Computer records showed a single login to Defendant's network account following a meeting during which he was put on leave. After careful review, we hold that under the Cherokee Code, evidence of an unauthorized login, without more, is insufficient to convict for the misuse of Tribal property. Because the Tribe failed to provide evidence of appropriation of Tribal property for Defendant's own use or use of another, as required by the Cherokee Code, we vacate Defendant's conviction.

I. FACTUAL AND PROCEDURAL HISTORY

Defendant Benjamin Cody Long ("Defendant") was charged on 2 March 2020 with seven (7) counts of Misusing Tribal Money or Property (C.C. § 14-70.42). The offenses were alleged to have occurred on 5 December 2019 (20 CR 464-465), 6 December 2019 (20 CR 466-467), and 7 December 2019 (20 CR 468-470). On 26 July 2021, the Eastern Band of Cherokee Indians ("EBCI" or "Tribe") filed a statement of charges in 20 CR 464 and 20 CR 465. On 9 August 2021, the Tribe dismissed with leave the charges in 20 CR 466-470. Defendant had been charged with two (2) counts related to a December 2019 ransomware attack (19 CR 2405-2406), but these charges were dismissed on 17 February 2021. At trial, the Tribe voluntarily dismissed the charges in 20 CR 464, and the case proceeded on a single count of misusing Tribal property, C.C. § 14-70.42(c)(1), stemming from unauthorized access of the Tribal computer network at 8:26 A.M. on 5 December 2019, as charged in 20 CR 465.

The evidence presented at trial tended to show the following:

At the time of the alleged offense, Defendant was employed by the Tribe as the lead systems administrator for the Office of Information and Technology ("IT Department"). Between 8:00 A.M. and 8:15 A.M. on 5 December 2019, William Travitz ("Travitz"), the head of the IT Department, and Anthony Brown ("Brown"), Defendant's direct supervisor, met with Defendant to inform him that he was being placed on paid administrative leave pending investigation into his prior accumulated employment infractions. After meeting with Defendant, Travitz and Brown collected Defendant's Tribal credentials, account information, employee badge, and laptops.

However, Defendant did not then return the cell phone SIM card provided to him by the Tribe, as he stated he had left his cell phone at home. Other IT workers testified that this was unusual, since possessing their phones at work was required in order to perform multi-factor authentication allowing login to network accounts.[1] Defendant returned at some time after 9:00 A.M. and turned in the SIM card.

As lead systems administrator, Defendant had access to multiple high-level EBCI network accounts. The account assigned to him was the Domain Administrator Account, also known as the Tribe's "god account," and he also had access to the shared "Serve Admin" account. Both accounts had broad access to nearly all services and resources on the Tribal network. Defendant's Domain Administrator Account was disabled at approximately 8:30 A.M. on Thursday, 5 December 2019, but Travitz planned to change the Serve Admin Account password over the weekend to avoid disrupting network services reliant on that account.

Doug Chase, the Tribe's Information Security Officer, reviewed the Tribe's Microsoft Azure logs as part of a separate investigation into an event affecting the Tribal network. The Tribe's Microsoft Azure logs tracked logins to Windows accounts on the Tribal network. They recorded two logins to Defendant's Domain Administrator Account on the morning of 5 December, at 8:04 A.M. and 8:26 A.M. The second of these logins occurred after Defendant's meeting with Travitz and Brown but before his access was disabled. Both logins were performed using Windows

[1] Multifactor authentication is a security technique that requires the user attempting to log in to confirm their identity using a second form of contact, usually email, SMS, or an authentication application.

Hello, a login method that was disabled on Tribal computers. This indicated to investigators that the login was performed using a computer or mobile device not owned by the Tribe. Each login was performed with multifactor authentication, and the Azure login records indicated that this authentication was done via SMS, or text message, to a cell phone. The authentication methods enabled on Defendant's account were (1) email and (2) text message to the cell phone number issued to Defendant by the Tribe. The 8:26 A.M. login to Defendant's account, performed after Defendant was informed that he was being placed on paid administrative leave, is the basis for the charge of appropriating Tribal property under C.C. § 14-70.42.

Defendant did not testify at trial, and his evidence was limited to that of his expert witness, Clark Walton ("Walton"). Walton testified that, in his opinion, the 8:26 A.M. login was performed by Josh Oliver, an IT employee who was asked to check the status of Defendant's remote access to Tribal computers.

At the close of the Tribe's case-in-chief, Defendant moved for a judgment of acquittal based on insufficiency of the evidence presented to meet the elements of the charge. Defendant renewed this same motion for judgment of acquittal prior to jury instruction and deliberation, thereby preserving for appeal the issue of sufficiency of the evidence in accordance with Rule 9(b)(3) of our Rules of Appellate Procedure. The trial court denied Defendant's motion both times. Defendant was convicted by jury of violating C.C. § 14-70.42 and sentenced to 454 days' imprisonment, with credit for 454 days' time served.

Defendant appeals, arguing the lower court erred in denying his motion for judgment of acquittal, failing to properly instruct the jury as to the meaning of the word "appropriate" as used in the code provision, and allowing a lay witness to provide expert testimony.

II. DISCUSSION

On appeal, Defendant alleges, among other arguments, that the trial court erred in denying his motion for judgment of acquittal because the Tribe failed to produce evidence to prove the necessary elements of the crime of appropriating Tribal property for his own use or that of another. We agree. Because we hold that the Tribe failed to provide evidence of one element of the offense, we need not address other issues raised by Defendant.

A. Standard of Review

In determining the standard of review, we are "bound by the laws, customs, traditions, and precedents of the [EBCI]. If there is no applicable Cherokee law, the Judicial Branch shall look next to Federal law, then to North Carolina law, and finally to the law of other jurisdictions for guidance." C.C. § 7-2; *Eastern Band of Cherokee Indians v. Martinez*, 15 Am. Tribal Law 45, 47 (2018).

"Whether the [Tribe] presented substantial evidence of each essential element of the offense is a question of law; therefore, we review the denial of a motion to dismiss de novo." *State v. Crockett*, 368 N.C. 717, 720, 782 S.E.2d 878, 881 (2016). In ruling on a motion to dismiss for insufficient evidence, we consider the evidence in the light most favorable to the Tribe, drawing all reasonable inferences and resolving

any contradictions or conflicts in the evidence in the Tribe's favor. *State v. Miller*, 363 N.C. 96, 98, 678 S.E.2d 592, 594 (2009).

B. Motion for Judgment of Acquittal

Defendant was convicted of the offense of misusing Tribal property:

> It shall be unlawful for a person in possession of or charged with the safekeeping, transfer or use of Tribal property to: (1) Without lawful authority appropriate the Tribal property or any portion of it to his own use or use of another[.]

C.C. § 14-70.42(c)(1). In order to convict under this provision of the Cherokee Code, the Tribe must show that (1) Defendant was in possession of or charged with the safekeeping of Tribal property; (2) he appropriated the Tribal property to his own use or use of another; and (3) he did so without lawful authority. For a first offense, the Cherokee Code authorizes punishment of up to three years' imprisonment, a fine up to $15,000, exclusion for five to ten years, or a combination of any of these punishments. *Id.* § 14-70.42(d). For a second or subsequent conviction, exclusion may be imposed for not less than ten years. *Id.*

On appeal, Defendant makes several arguments regarding whether his conduct falls under the Cherokee Code's prohibitions, in particular that (1) because he was on leave he was no longer "in possession of or charged with the safekeeping" of Tribal property, and (2) he did not "appropriate" Tribal property because he did not exclude the Tribe from its property.

We need not reach these arguments. The primary question before the Court is whether the Tribe's evidence met the statutory element that requires a defendant

"appropriate the Tribal property . . . to his own use or use of another." C.C. § 14-70.42(c)(1). The Tribe argues that under the statute, a *de minimis* intrusion into the Tribe's network, without evidence of Defendant's purpose or of further conduct, constitutes an appropriation of Tribal property for Defendant's own use or use of another. We disagree. Even assuming Defendant's conduct constituted an appropriation, the Tribe failed to produce any evidence showing Defendant put the network to his own use or that of another.

Taken in the light most favorable to the Tribe, the evidence shows that Defendant logged into his administrator-enabled account after he was placed on leave and was instructed not to access network resources. The Tribe provided no evidence that Defendant obtained information, downloaded data, changed settings, or installed or ran software: the evidence showed no conduct beyond simply logging into the account without permission. Further, there was no evidence of the use to which Defendant put Tribal property. We must determine if the Tribal Council intended to criminalize Defendant's conduct and punish it as a felony.

This inquiry presents a question of statutory interpretation. Issues of statutory interpretation are reviewed *de novo;* the Court "determine[s] the meaning that the [Tribal Council] intended upon the statute's enactment." *State v. Dudley*, 270 N.C. App. 771, 773, 842 S.E.2d 163, 164 (2020) (internal quotation and citation omitted). If the statutory language is clear and unambiguous, we "eschew[] statutory construction in favor of giving the words their plain and definite meaning." *State v. Beck*, 359 N.C. 611, 614, 614 S.E.2d 274, 277 (2005). When the statute is ambiguous,

we use judicial construction to determine the legislative intent. *Id.* We generally construe criminal statutes against the Tribe, as the rule of lenity requires us to strictly construe ambiguous criminal statutes. *See State v. Hinton,* 361 N.C. 207, 211, 639 S.E.2d 437, 440 (2007) ; *State v. McGaha*, 306 N.C. 699, 702, 295 S.E.2d 449, 451 (1982). However, this does not mean that words are given "their narrowest or most strained possible meaning." *Beck*, 359 N.C. at 614, 614 S.E.2d at 277. "A criminal statute is still construed utilizing common sense and legislative intent." *Id.* (internal quotation and citation omitted). For the rule of lenity to apply, there must be more than one "plausible reading that comports with the legislative purpose in enacting [the statute]." *See State v. Abshire*, 363 N.C. 322, 332, 677 S.E.2d 444, 451 (declining to apply the rule of lenity after determining that there was only one plausible construction of the statute).

In this case, the ambiguity at issue stems from the second element of the offense, Defendant's "appropriat[ion of]] the Tribal property or any portion of it to his own use or use of another." C.C. § 14-70.42(c)(1). Two questions arise in determining whether Defendant's conduct falls under the Cherokee Code's proscriptions. First, did Defendant appropriate the Tribal property by simply logging in without authorization, or is the Tribe required to show that he committed some further act, such as copying or deleting data from the network or installing software, in order to show that an appropriation occurred? Second, if Defendant's conduct does constitute an appropriation, did the Tribe show that Defendant appropriated Tribal property "to his own use or use of another?" Our analysis hinges on this second question.

Reviewing the plain language of the Cherokee Code and other jurisdictions' interpretations of their terms of art, we hold that the Tribe must show more than the *de minimis* fact of logging into the network to satisfy its burden of showing that Defendant's appropriation of Tribal property was to his own use or use of another.

The Tribe has provided no evidence of the use to which Defendant put Tribal network resources. While the proper definition of "appropriate" was disputed at trial and on appeal, because our holding is based on the Tribe's failure to present any evidence showing that Defendant put the Tribe's property "to his own use or use of another," we need not determine whether an unauthorized login constitutes an appropriation. Even assuming Defendant's conduct constitutes a misappropriation of property, the Tribe has failed to show that this appropriation was for Defendant's own use or that of another, as it produced no evidence of Defendant's intent or of further conduct once he obtained access to the Tribal network.

We note initially that under a plain reading of the text, the inclusion of "to his own use or use of another" in an element of the criminal statute implies that there must be some evidence of the use to which Defendant put the appropriated property. "Since a legislative body is presumed not to have used superfluous words, our courts must accord meaning, if possible, to every word in a statute." *C Investments 2, LLC v. Auger*, 383 N.C. 1, 12, 881 S.E.2d 270, 279 (2022) (internal quotation and citation omitted). With no direct evidence of Defendant's intent upon logging into the network, or what, if any, use to which he put the network after logging in, the question becomes whether the plain fact of his logging in raises an inference that Defendant put Tribal

network resources to his own use or the use of another. We do not believe that such an inference is reasonable.

A review of the use of this terminology in other contexts tends to support our conclusion. When a lawmaking body borrows a term of art, we presume that it adopts the "cluster of ideas" associated with that term. *Morissette v. U.S.*, 342 U.S. 246, 263, 72 S.Ct. 240, 250 (1952). The language of appropriating for one's own use appears from time to time in other jurisdictions' statutory contexts, perhaps most commonly in embezzlement statutes roughly parallel to Cherokee Code § 14-70.42. In these other contexts, the question of whether the defendant's appropriation put the property to his own use or that of another is rarely at issue. For example, the federal government prohibits agents of bankruptcy estates from fraudulently appropriating to their own use any property belonging to the estate. 18 U.S.C. § 153. Although North Carolina's General Statutes do not use identical language of misappropriation, they prohibit one entrusted with property from "embezzl[ing] or fraudulently . . . misapply[ing] or convert[ing] [it] to his own use." N.C. Gen. Stat. § 14-90(b)(1) (2023). Case law involving those statutes generally involves the unauthorized transfer of funds or property to the control of the defendant. *See, e.g.*, *United States v. Bennett*, 874 F.3d 236, 258 (5th Cir. 2017) (holding evidence that defendant had access to bankruptcy estate's accounts and fraudulently appropriated property from estate to her personal account was sufficient to support bankruptcy fraud conviction); *State v. Steele*, 281 N.C. App. 472, 481-82, 868 S.E.2d 876, 883 (holding evidence that fiduciary withdrew and used funds for personal benefit was sufficient to support

conviction for embezzlement), *disc. review denied*, 878 S.E.2d 809 (N.C. 2022). In those cases, the defendants took possession of funds or other property and deprived the rightful owner of control, making clear that the appropriation was for their own use. It is unclear from precedent whether the courts of those jurisdictions would recognize Defendant's unauthorized login as an appropriation "to his own use or use of another," with no evidence of what that use was or that he or someone else benefited from the appropriation.

Part of the difficulty in this case is the translation of legal concepts traditionally concerned with money or physical property to the context of digital access. Perhaps more instructive are cases in which courts have applied those concepts to less concrete property rights, like those stemming from intellectual property. For example, the Restatement of Torts recognizes a cause of action for "appropriat[ing] to his own use or benefit the name or likeness of another." Restatement (Second) of Torts § 652C (1977). North Carolina recognizes this tort as the "appropriation of a plaintiff's name or likeness for a defendant's advantage." *Miller v. Brooks*, 123 N.C. App. 20, 25, 472 S.E.2d 350, 353 (1996), *disc. review denied*, 345 N.C. 344, 483 S.E.2d 172 (1997). North Carolina also recognizes the tort of misappropriation of trade secrets, with misappropriation in that context defined as the "acquisition, disclosure, or use of a trade secret of another without express or implied authority or consent." N.C. Gen. Stat. § 66-152(1) (2023).

In either of these intellectual property contexts, there must be some showing beyond the simple fact of appropriation in order for liability to attach. For example,

misappropriation of likeness requires a showing of intent: a law firm did not misappropriate the likenesses of two former employees where the firm removed links referring to the defendants from the firm website—even though html code files remained on a server not owned by the firm—because no evidence was presented to suggest that the firm intended to preserve a copy of the deleted files. *Merritt, Flebotte, Wilson, Webb & Caruso, PLLC v. Hemmings*, 196 N.C. App. 600, 613, 676 S.E.2d 79, 89, *disc. review denied*, 363 N.C. 655, 686 S.E.2d 518 (2009).

Perhaps more directly analogous to this case: the mere opportunity to misappropriate trade secrets is not sufficient to create liability. *See RLM Commc'ns, Inc. v. Tuschen*, 831 F.3d 190, 200 (4th Cir. 2016). Although North Carolina's statute addressing the misappropriation of trade secrets only explicitly places the burden on an employer to show that an employee "knows or should have known of the trade secret" and "had a specific opportunity to acquire it for disclosure or use or has acquired, disclosed, or used it" without the consent of the owner, N.C. Gen. Stat. § 66-155 (2023), the Fourth Circuit has held that showing only opportunity is insufficient, and an employer must "raise an inference of actual acquisition or use of trade secrets to survive summary judgment." *RLM*, 831 F.3d at 202. North Carolina courts have recognized a similar requirement. *See, e.g., Modular Techs., Inc. v. Modular Sols., Inc.*, 184 N.C. App. 757, 646 S.E.2d 864, 2007 WL 2034046 at *4 (2007) (unpublished) (finding no liability because the plaintiff had not introduced substantial evidence that the defendant actually acquired the information for disclosure or use or that she

disclosed or used the information).[2] Simply having access to confidential information and the opportunity to acquire it for her own use did not, without additional evidence, give rise to an inference that the defendant did so. *Id.* at *5.

Though these types of claims are different from the provision of the Cherokee Code we are evaluating and cross boundaries between criminal and civil contexts, they are helpful in defining boundaries of what conduct constitutes appropriation of property "to [one's] own use or use of another." Without evidence of any use to which Defendant put Tribal property, we cannot uphold his conviction due to the absence of an essential element of the crime.

We note that our decision does not imply that Section 14-70.42(c)(1) can never apply to computer crimes. Had the Tribe provided evidence of Defendant's intent while accessing the network or that he had installed software, accessed files, or otherwise actually made use of his access, that evidence may have been sufficient to show that Defendant's appropriation of Tribal property was "to his own use or use of another." In this case, the Tribe simply failed to carry its burden on that element.[3]

III. CONCLUSION

For the foregoing reasons, we hold that the trial court erred in failing to grant Defendant's motion for acquittal, and we vacate Defendant's conviction.

---

[2] Although unpublished opinions are binding on neither North Carolina courts nor on this Court and therefore citation is generally discouraged, this matter appears rarely before the courts, and we find the reasoning of the North Carolina Court of Appeals in *Modular Techs*, adopted by the Fourth Circuit in *RLM*, to be compelling.

[3] If the Tribal Council wishes to directly address misconduct involving computer access, we respectfully suggest it adopt a computer crime code provision as have other jurisdictions (e.g., North Carolina's Article 60. N.C. Gen. Stat. §§ 14-453-59 (2023)).

Because we are vacating Defendant's conviction, we do not address Defendant's additional arguments.

VACATED.

Kirk Saunooke

Chief Justice

Brenda Toineeta Pipestem

Associate Justice

Robert Hunter

Associate Justice