Access DENIED?

THINK TWICE BEFORE SHARING YOUR DEVICE'S PASSCODE.

WRITTEN BY **PIERRE GROSDIDIER**

SERVICEMEMBER ETHEN BLACK LEARNED THE HARD WAY that sharing a phone passcode with another without express restrictions effectively grants this person and others unfettered access to the device.[1] Black lent his phone to a fellow soldier for a night shift with the agreement that the latter would use it to call and text his girlfriend, stream YouTube, and play a designated game. Black did not otherwise expressly restrict the soldier's use of the phone. The soldier stumbled upon objectionable photos of otherwise clothed fellow female soldiers, civilians, and children in the phone's unprotected photo gallery. The soldier handed the phone unlocked to a sergeant who viewed the photos and others, in another folder, that he believed to be child pornography. The sergeant immediately closed the folder, returned the phone to the soldier, and reported the incident. Placed in custody, Black consented to a phone search in writing, which revealed suspected child pornography.[2]

The military judge overseeing Black's general court-martial for possession of child pornography granted a motion to suppress the evidence on the basis of search consent and scope arguments.[3] The U.S. Army Court of Criminal Appeals reversed. The court grounded its argument on the premise that "[v]oluntary consent to search is a well-recognized exception to the [Fourth Amendment's] warrant requirement."[4] Moreover, consent can be granted by a third party who possesses common authority over the property subject to the search.

As to the soldier's initial search, the court held that Black granted him unfettered access to the phone because Black provided the passcode, did not encrypt or protect the photos, and did not expressly restrict the phone's use beyond those uses Black consented to. Common authority law, the court held, does not require an owner to authorize each use of a device or each access to its folders. What counts are the expressed restrictions. In their absence, as in this case, the owner assumes the risk that the other person will explore every part of the device and even share its contents with others.[5]

The court also rejected Black's argument that the sergeant, who was acting in his official capacity, exceeded the scope of the soldier's consent to search Black's phone. Consent to search a space, like a car, extends to containers within that space.[6] Likewise with computers and attached peripheral devices. In this case, the soldier handed the unlocked phone to the sergeant without restrictions to verify the existence of inappropriate photos. Viewing this exchange objectively, a reasonable person would have construed it to give the sergeant free reins to peruse the phone for photos, including those in folders not seen by the soldier.[7]

U.S. v. Black is consistent with *People v. Davis*.[8] Shaun Davis asked a police officer to call his girlfriend to come and pick up her car, which he had borrowed to commute, after he was arrested at work. Davis compliantly provided his passcode and phone to facilitate the call, without otherwise placing any restrictions on the passcode's use. The police secured a warrant and used the passcode to access and search the device. Davis successfully moved the trial court to suppress the fruits of the phone's search, but the Colorado Supreme Court reversed in an interlocutory appeal. It held that Davis did not manifest a subjective expectation of privacy in the passcode when he shared it with an arresting officer and that, even if he did, society would not recognize it as reasonable under the circumstances.[9] Moreover, once handed over to the government, Davis could not expect the passcode to remain private regardless of any limitations Davis might have "*implicitly* placed on the disclosure."[10] **TBJ**

NOTES

1. *United States v. Black*, Army Misc. 20210310, 2021 WL 4953849, at *1 (A. Ct. Crim. App. Oct. 22, 2021).
2. *Id.* at **1–2.
3. *Id.* at **2–3.
4. *Id.* at *4.
5. *Id.* at **5–6.
6. *Id.* at *6.
7. *Id.* at *7.
8. 438 P.3d 266, 267 (Colo. 2019).
9. *Id. at* 271; *see generally Katz v. United States,* 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (Fourth Amendment analysis inquires whether a person has manifested a subjective expectation of privacy that society is willing to recognize as reasonable).
10. *Id.* (emphasis added).

PIERRE GROSDIDIER is an attorney in Houston. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Grosdidier's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, he worked in the process control industry. Grosdidier holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section chair-elect for 2021-2202.