Published on *The National Law Review* https://natlawreview.com

New Georgia Decision Clarifies Scope of Computer Trespass Statute

Article By:

Todd Van Dyke

Just as the United States Supreme Court recently limited the reach of the federal Computer Fraud and Abuse Act ("CFAA") in *Van Buren v. United States*, the Georgia Supreme Court has now reined in the Georgia state law counterpart to the CFAA.

Background

In *Kinslow v. State*, No. S20G1001 (June 21, 2021), the defendant was an IT employee of the City of Norcross. The defendant allegedly altered the City's computer network settings to cause his boss's incoming emails to be copied and forwarded to the defendant's personal email account. The jury found the defendant guilty of state-law computer trespass, and the defendant appealed.

The Georgia computer trespass statute defines the offense, in part, as "us[ing] a computer or computer network with knowledge that such use is without authority and with the intention of . . . [o]bstructing, interrupting, or in any way interfering with the use of a computer program or data." OCGA § 16-9-93(b)(2) (emphasis added).

No "Obstruction" or "Interference" in Copying Emails

There was no question the defendant in *Kinslow* lacked the authorization to access and forward his boss's emails. But the majority concluded that the evidence at trial could not prove the defendant acted "with the intention of obstructing or interfering with the use of data."

Relying on dictionary definitions of the words "obstruct" and "interfere," and applying the canons of construction, the court interpreted the statute as requiring proof that the defendant "hindered" the use of data in some way. According to the court, the evidence showed, at most, the defendant enabled a copy of computer data to flow to another recipient. Because "[t]here [was] no evidence that [the defendant] by his actions hindered the flow of data to any intended recipient or otherwise hindered the use of data," the court overturned the conviction for computer trespass under the Georgia statute.

The majority ruling drew a sharp dissent. The dissent would have held the defendant's actions to "manipulate" the data stream and "intermeddle" data intended to go to others satisfied the "in any

way interfering" provision of the statute. The dissent reasoned, "[T]respass does not require the theft of data from its intended recipient—it requires only that one accesses that data from a place one is not authorized to be." (This interpretation would have tracked the CFAA, which prohibits merely "obtain[ing]" information without authorization.)

Takeaways

The dissent warned that this decision "educates wrongdoers that they are better off from both a detection standpoint and from prosecution as a matter of law if they simply copy data rather than block its delivery." At least for application of the Georgia computer trespass statute, that point is hard to argue. That said, the defendant's alleged conduct here might have violated a host of other laws, including the CFAA and possibly trade secret laws.

Employers should keep in mind that many states have computer trespass statutes that do not necessarily rise and fall with the CFAA. Some may be broader, and some, like Georgia's, may be narrower. Whenever an employee accesses information to which the employee lacks authorization, or improperly uses information to which access is authorized, employers should work with counsel to carefully analyze the possible legal implication of such conduct.

National Law Review, Volume XI, Number 175