

MDM&C Update

[Click Here to Learn More About MDM&C >](#)

May 15, 2020

IS UNAUTHORIZED USE OF A WORK COMPUTER A CRIME? U.S. SUPREME COURT TO DECIDE

With many employees working from home a number of issues have become more pressing, including misuse of an employer's computer system. The Computer Fraud and Abuse Act criminalizes "obtaining information from any protected computer" by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access." But what if an employee is authorized to access the computer and accesses the computer for an illicit or improper purpose? For example, an employee is authorized to access the employer's computer, but does so to misuse the employer's trade secrets.

The United States Supreme Court has agreed to hear a case that will resolve the issue, *United States v. Van Buren*. The facts in *Van Buren* are colorful. Van Buren, who was a sergeant in a local police department in Georgia, became acquainted with a recent widower in his early sixties, who fancied young women and often sought the services of prostitutes. He allegedly paid the prostitutes to spend time with him and then accused them of stealing from him. Although warned to steer clear of the widower by his supervisors, Van Buren developed a relationship with him. Van Buren's initial contact with the widower came when he arrested him for providing alcohol to a minor, but over time he began to mediate disputes between the widower and young women.

Van Buren had financial difficulties and saw the widower as the solution. Van Buren told the widower that he needed a loan of \$15,368 to cover medical bills for his son. There was no such bill. The widower taped the conversation and gave it a detective, claiming that Van Buren was trying to shake him down. The FBI became involved and a sting was arranged.

The widower told Van Buren that he wanted him to run a check on a license plate of a woman he met at a strip club. He wanted to make sure that she was not an undercover police officer before he continued his relationship with her. Van Buren agreed to run the plate for a thousand dollars and did so. But the plate was a phony created by the FBI as part of its sting.

Van Buren was arrested and convicted of violating the Computer Fraud and Abuse Act. He appealed, arguing that he was authorized to access the database that had the license information. The 11th Circuit rejected his argument and held that although he was authorized to access the information, he was authorized to do so only for law enforcement purposes, and not for his personal benefit. By doing so he exceeded his authorized access and, therefore violated the law.

The question of whether an individual "exceeds authorized access" to a computer when he alters or obtains information he is authorized to access, but for an improper or illicit purpose, has sharply divided the courts. For example, the Second Circuit has held that a violation of the Computer Fraud and Abuse Act only occurs when an individual obtains or alters information on a computer that the individual is not

authorized to access for any purpose.

In *United States v. Valle*, a New York City police officer, living with his wife and infant daughter, was an active member of an internet sexual fetish community. He communicated with individuals by email and web chat and exchanged photographs of women he knew, including his wife, and discussed “committing horrific acts of sexual violence” on these women. The chats included “graphic descriptions of kidnapping, torturing, cooking, raping, murdering and cannibalizing various women,” whose photographs had been exchanged among the members of the sexual fetish community.

Valle’s wife, concerned about his late night on-line activities, discovered some disturbing photographs on the computer that they shared. She installed spyware and when the full extent of her husband’s activities were revealed, she moved out of their house and contacted federal authorities.

Investigating Valle, federal authorities discovered that he had accessed databases available for law enforcement purposes to get personal information about a woman he knew and had fantasized committing violent sexual acts on her. Valle admitted, as he must, that he had no legitimate reason to access the database and doing so was a clear violation of his employer’s policies. But he argued that since he was an authorized user, he could not have violated the Computer Fraud and Abuse Act.

The Second Circuit, whose decisions are controlling in New York, Connecticut and Vermont, agreed. It held that if an employee has access to the computer, the employee does not violate the Act, even if the employee accesses it for a purpose prohibited by the employer. Thus, the *Valle* court held that the Act could only be violated by one who is not authorized to access the computer for any purpose.

Now the Supreme Court will decide whether an individual, who has access to a computer, commits a crime by accessing that computer for an illicit or improper purpose, as the *Van Buren* court held, or whether the Act is limited to accessing a computer for which the individual is not authorized for any purpose, as the *Valle* court held.

However the Supreme Court resolves the issue, employers are well advised to establish clear policies on the permissible use of the employer’s computer system and the use of information to which the employee is granted access.

If you have any questions about this or any other employment issue, please feel free to contact **Bernard E. Jacques** at bjacques@mdmc-law.com.

Offices

NEW JERSEY | NEW YORK | COLORADO | PENNSYLVANIA
CONNECTICUT | MASSACHUSETTS | DELAWARE | RHODE ISLAND | FLORIDA

The information provided in this Newsletter should not be relied upon as legal advice or a legal opinion on any specific set of facts or circumstances. The contents are intended for general information purposes only and you are urged to consult an attorney concerning your own situation and any specific legal questions you may have. This Newsletter may be considered Advertising under the court rules of certain states.

© COPYRIGHT 2020 McELROY, DEUTSCH, MULVANEY & CARPENTER, LLP. ALL RIGHTS RESERVED.